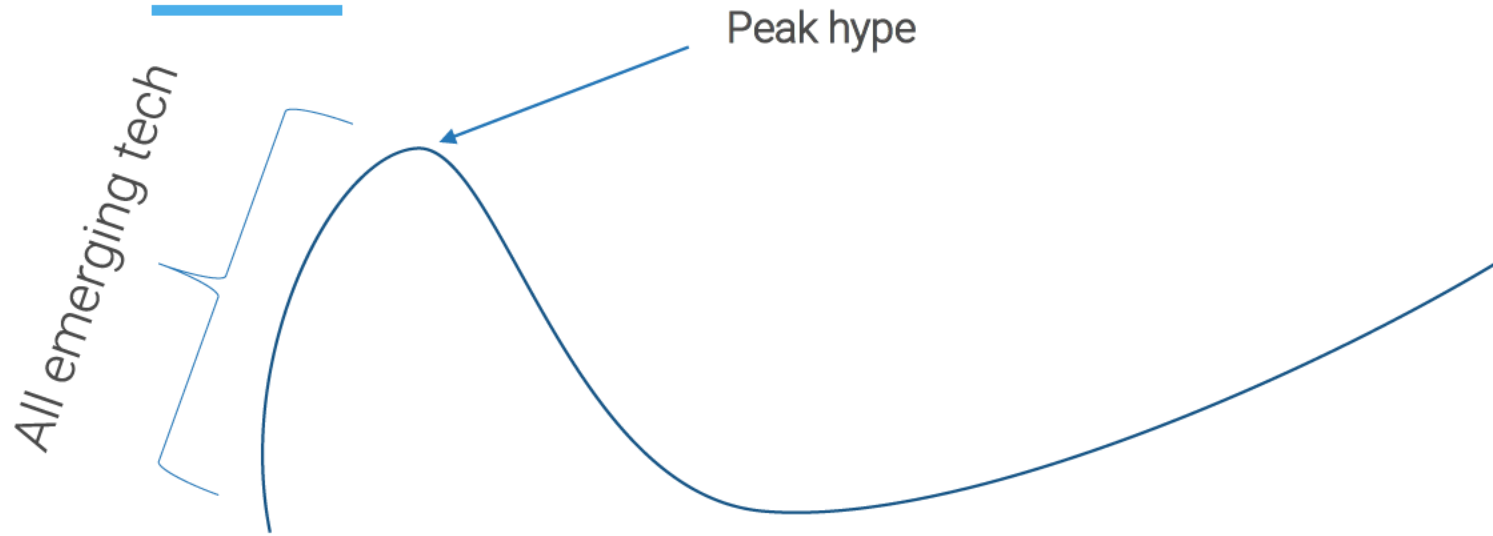


Beyond the Hype: Emerging Technologies in 2023

Presented by

Brian Jackson

Are all emerging technologies merely hype?



Looking deeper

- Push past the hype
- What can help us grow?
- What will protect us?

3 technologies to accelerate growth

2 technologies for protection

Grow

Metaverse

Generative AI

Private Network Services

2023 investment %

13% will invest in XR headsets

48% will invest in AI

15% will invest in 5G

Protect

Transparency Ledgers

ESG Analytics

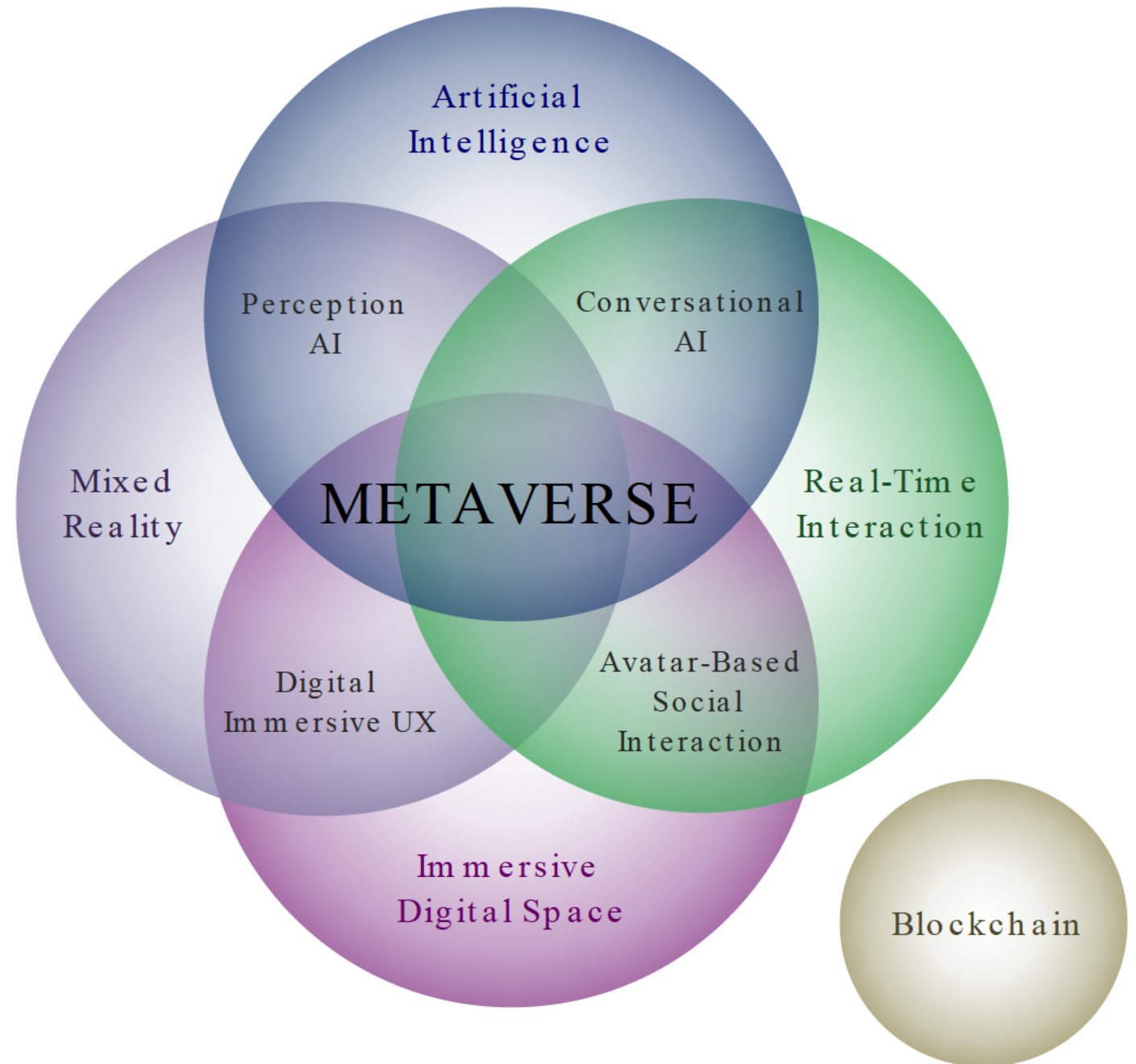
41% will invest in next-gen cyber sec

15.3% will invest in ESG metrics reporting



The metaverse is a technological convergence

- User **presence** is represented
- The world is **persistent**
- Data is **portable**



Most IT pros have no interest, and no plans to use virtual reality collaboration

How interested are you in using a virtual reality headset to collaborate with your colleagues?

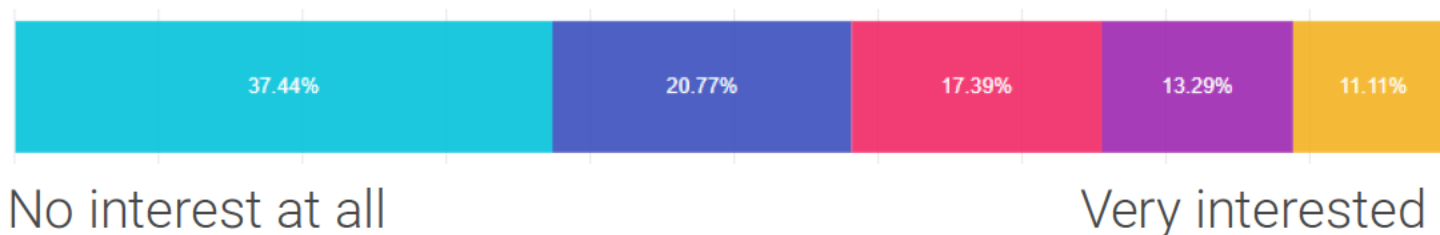


Image generated by Midjourney with prompt:

artificial consciousness, surreal, futuristic, dystopian

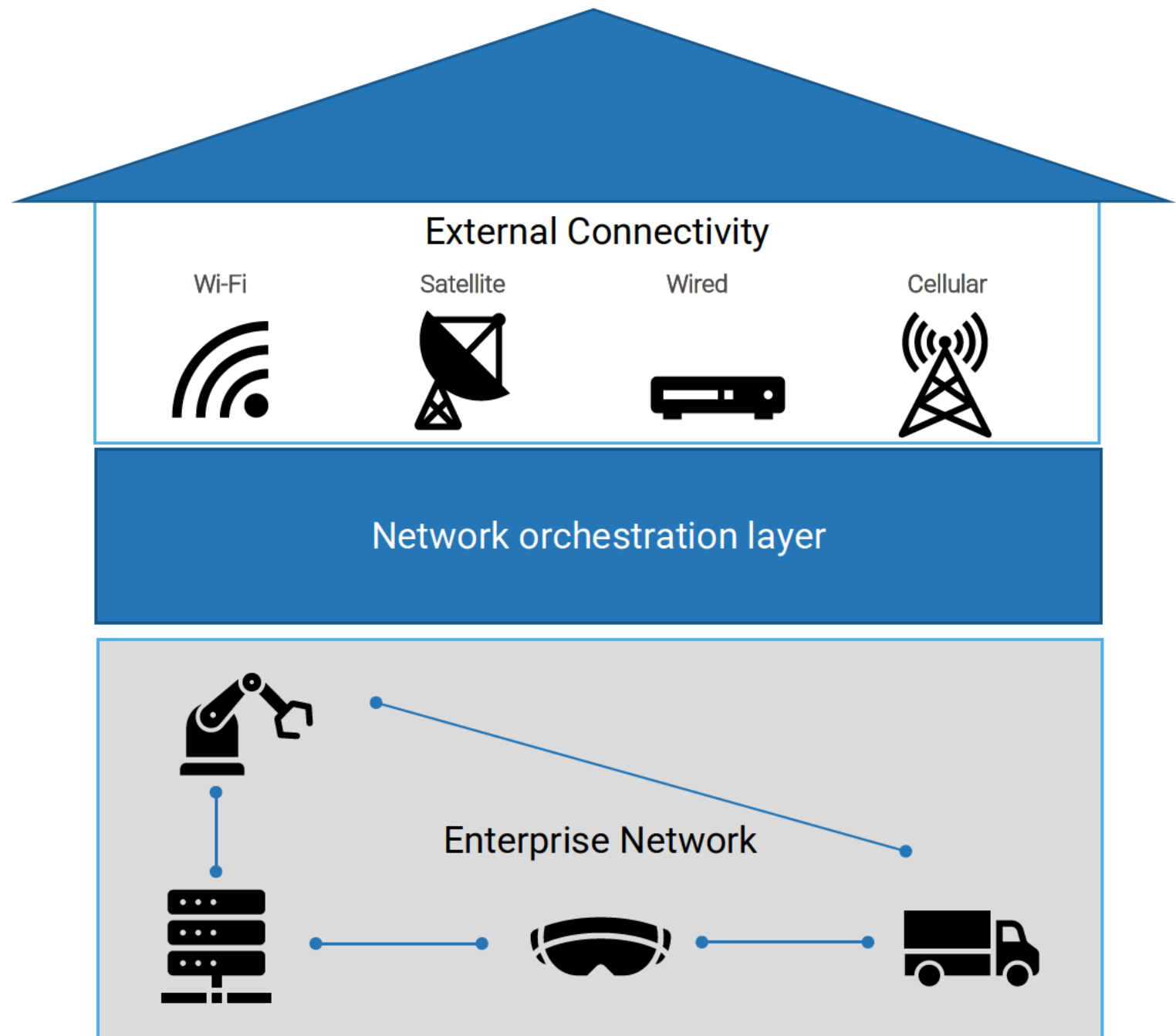


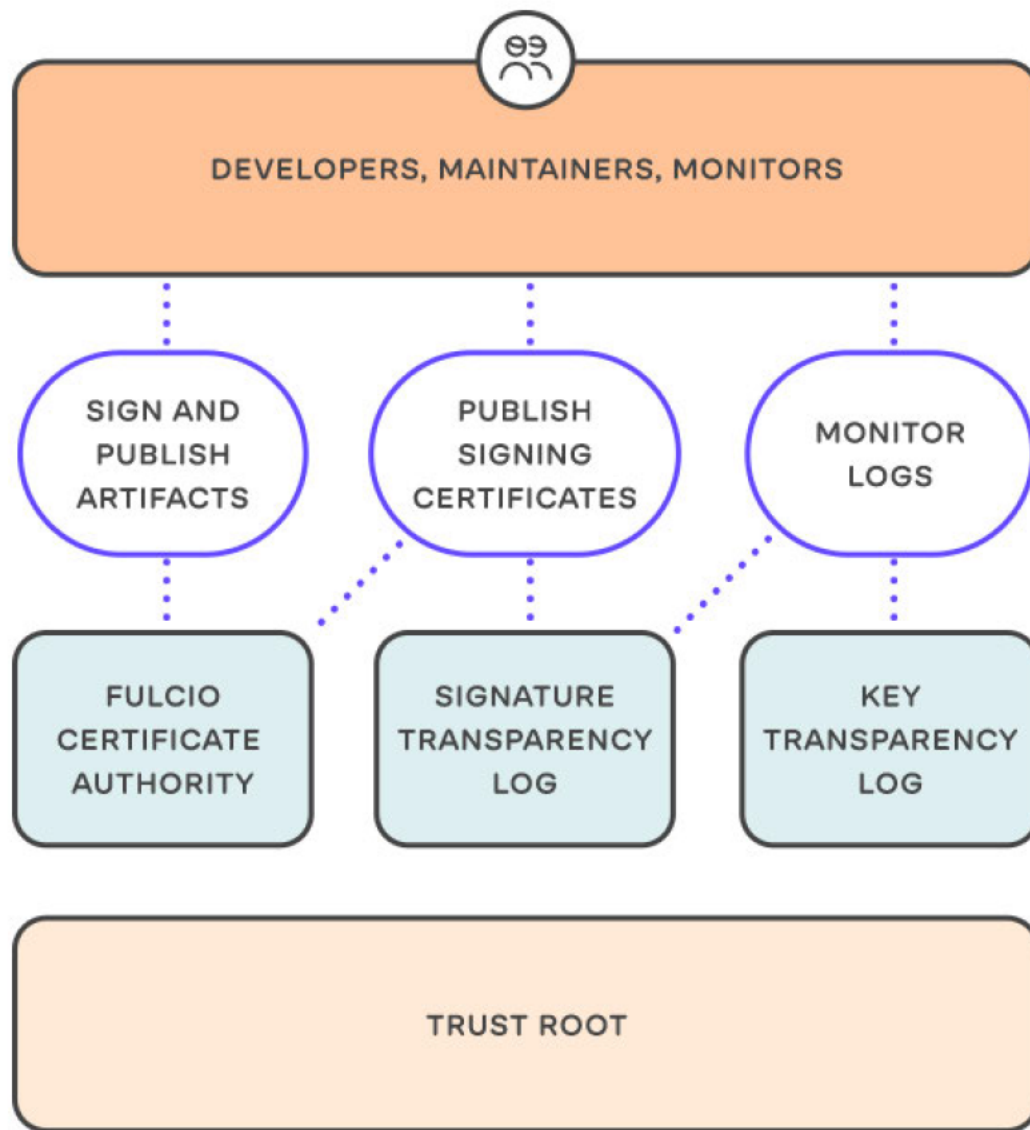
Generative AI accelerates creativity

Algorithms trained to generate content that is meaningful to humans will inspire new business models.

Private Network Services improve connectivity

Enterprise networks are being taxed to keep up with bandwidth demands and number of connected devices. A new network orchestration layer will help take advantage of private network access options like 5G cellular.





Transparency Ledgers enable zero trust security

Making software assets traceable from artifact back to the original code is crucial to secure the supply chain

Sigstore is a solution that brings together free technologies to make open source software safer.

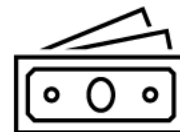
ESG Analytics

Reporting on carbon emissions and other environmental, social, and governance metrics to satisfy investors and regulators.

New Criteria For Market Capitalization



Statement Of
Quarterly Financial
Performance

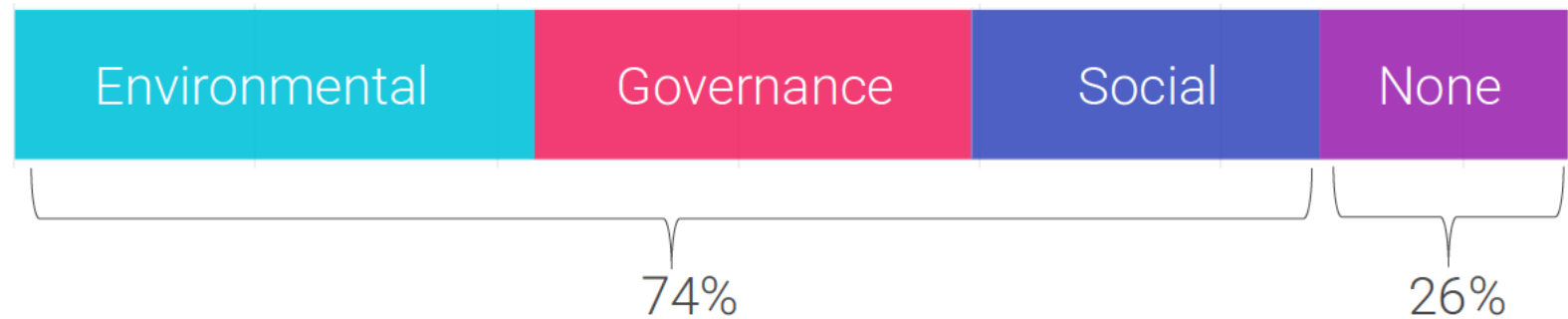


Statement Of
Quarterly ESG
Performance



Most IT departments are supporting an ESG initiative in 2023

Is IT planning to support any environmental, social, or governance (ESG) mandates at the organization in the coming year?



Investigating 2023 Tech Trends



Analyst Braintrust

Brainstorming
and conversation
with Info-Tech
analysts.



Survey Data

Survey to our
community of IT
decision makers.



Case Studies

Real examples of
technologies in
the field.



Diagnostics

Benchmark data
from Info-Tech
clients.



PURPOSE

This form will be used to request and approve TS&CS deliverable activities. It will be saved in central repository (and automated as soon as possible).

CONTENTS

1. TS&CS INITIAL REQUEST	1
2. TS&CS PROGRAM MANAGEMENT REVIEW	3
3. TS&CS CONTRACTOR SUPPORT RESOURCE REVIEW	4
4. TS&CS COR APPROVAL	5

1. TS&CS INITIAL REQUEST

Please send initial requests to:

- Sylvester Smith: sylvestser.smith@gsa.gov
- (b) (6) [gsa.gov](mailto:(b) (6)@gsa.gov)
- (b) (6) [gsa.gov](mailto:(b) (6)@gsa.gov)

Requestor Name: Michael Lee

Requestor Email: Michael.lee@gsa.gov

Office Name: GSA/FAS/ITC/ETS

Date Requested: 8/12/2022

Date Needed: 9/30/2022

Request Type: ☒ White Paper ☐ Document ☐ Web Page ☐ Service Guide
☐ Template

Request Description: White Paper – Artificial Intelligence (AI) in government

Deliverable Requirements: White Paper - AI in government Document

Topics covered in the paper should be: AI in government to include, Embedded AI Generative AI and AI Engineering

1. Executive Summary
2. Introduction
 - a. Description
3. Federal Guidance and Efforts Supporting (insert technology topic)
4. The Emerging (insert technology here) Landscape
5. Technical Specifications (including infographic)
6. Agency Network Modernization (how the technology topic supports modernization)
7. Infographic
8. Considerations for Leadership/Management (i.e. CIOs)



9. Use Cases

10. Suggested Actions for Agencies

11. FAQs

- a. short description of technologies or business activities this replaces and estimated sunseting of the technology (if applicable)
- b. estimated dates for availability of the product for government usage (e.g. 2025, 2030, currently being adopted),
- c. Value to the end user
- d. How to get it today?

12. GSA Is Here to Help

- a. If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at <https://gsa.gov/nspsupport> or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your (insert white paper topic). Thank you for reading!

Estimated paper length is _TBD_ pages or less and must be Section 508 compliant for accessibility.



2. TS&CS PROGRAM MANAGEMENT REVIEW

Please send requests to:

- (b) (6) jpidev.com
- (b) (6) jpidev.com

JPI Program Management Reviewer: First Name Last Name

Date Reviewed: 08/26/22022

Recommended For COR Approval? ☒ Yes ☐ No

Program Office Estimated LOE*: (Provide Hours)

NTE 125 Hours Across All LCATS

Report Level Definitions

Level 2 – Intermediate Complexity

Notes:

JPI believes this deliverable and the AI-as-a-Service should be consolidated and the hours used to complete the topics in both deliverables. Given there are a lot amounts of known unknowns, the Team recommends a two-week to one-month discovery phase to determine what AI services are available in GSA's suite of service offerings. As there are limited, if any, AI EIS CLINS to date, and the Team will do additional research into future service offerings to consider on EIS and if a Service Guide is prudent that this point of time.

This path forward was discussed with the TS&CS PM who agreed with the plan.

Bob Makowski will be the primary lead for this deliverable and will schedule a kick-off meeting once the initial research phase is complete to discuss next steps and a high-level project timeline.

The Team recommends a tentative completion date for this deliverable as 10/31/2022.



3. TS&CS CONTRACTOR SUPPORT RESOURCE REVIEW

TS&CS Support Staff Reviewer: (b) (6) on behalf of Bob Makowski

Date Reviewed: 08/26/2022

TS&CS Contractor Estimated Report Level(s): 110-125

Report Level Definitions

Level 2 – Intermediate Complexity

Notes:

The Project Lead agrees with the assumptions, recommendations, and path forward provided by the PM. Bob Makowski will complete an initial analysis, will provide a high-level report of available AI services, and a recommend project plan in a virtual meeting prior to 20 September 2022 followed by the activities outlined in the intake form for this deliverable and the service guide deliverable.



4. TS&CS COR APPROVAL

Email all approvals to:

- Sylvester Smith: sylvestser.smith@gsa.gov
- (b) (6) jpidev.com
- (b) (6) jpidev.com

TS&CS COR: Sylvester Smith

Date Reviewed: 08/30/2022

Approved for Production? ☒ Yes ☐ No

Appropriate Task Support Area:

☐ **Program Management Support**

Deliverable Name: Full Name of Report

☒ **Technical SME White Papers**

Report Levels: Level 2

**Note: for complex requests, it may be necessary to construct cost estimate by combining multiple report levels (e.g., working session for concept; initial draft; final report)*

☐ **Technical Requirements Development, Reports, and Webpage Updates**

Development Type: List Here

☐ **Service and User Guides**

Guide Type: List Here

Task Area Funding Available: ☒ Yes ☐ No

Approved Request Description:

White Paper - AI in government Document and if prudent AI-as-a-Service Service Guide

Notification Email Sent: ☒ Yes ☐ No

Notes (Schedule, Resources, etc.):

Tentative completion of 10/31/2022

Resources as identified above



PURPOSE

This form will be used to request and approve TS&CS deliverable activities. It will be saved in central repository (and automated as soon as possible).

CONTENTS

1. TS&CS INITIAL REQUEST	1
2. TS&CS PROGRAM MANAGEMENT REVIEW	3
3. TS&CS CONTRACTOR SUPPORT RESOURCE REVIEW	4
4. TS&CS COR APPROVAL	5

1. TS&CS INITIAL REQUEST

Please send initial requests to:

- Sylvester Smith: sylvestser.smith@gsa.gov
- (b) (6) gsa.gov
- (b) (6) gsa.gov

Requestor Name: Michael Lee

Requestor Email: Michael.lee@gsa.gov

Office Name: GSA/FAS/ITC/ETS

Date Requested: 8/12/2022

Date Needed: 9/30/2022

Request Type: ☐ White Paper ☐ Document ☐ Web Page ☒ Service Guide
☐ Template

Request Description: Service Guide – Artificial Intelligence (AI) as a Service

Deliverable Requirements: Service Guide - AI as a Service

Topics covered in the paper should be: AI as a Service

1. Executive Summary
2. Overview of Service
 - a. Description (including infographic)
 - b. Definition
3. Technical Specifications (including infographic)
4. Ordering Guidance (including infographic)
 - a. Pricing Basics
 - b. BIC Contracts
5. FAQs
6. References
7. GSA Is Here to Help



- a. If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at <https://gsa.gov/nspsupport> or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your (insert service guide topic). Thank you for reading!

Estimated paper length is _TBD__ pages or less and must be Section 508 compliant for accessibility.



2. TS&CS PROGRAM MANAGEMENT REVIEW

Please send requests to:

- (b) (6) jpidev.com
- (b) (6) jpidev.com

JPI Program Management Reviewer: First Name Last Name

Date Reviewed: MM/DD/YYYY

Recommended For COR Approval? ☐ Yes ☐ No

Program Office Estimated LOE*: (Provide Hours)

**Note: for complex requests, it may be necessary to construct cost estimate by combining multiple report levels (e.g., working session for concept; initial draft; final report)*

Report Level Definitions

Level 1 – Basic Complexity

Level 2 – Intermediate Complexity

Level 3 – High Complexity

Notes:

List Here



3. TS&CS CONTRACTOR SUPPORT RESOURCE REVIEW

TS&CS Support Staff Reviewer: First Name Last Name

Date Reviewed: MM/DD/YYYY

TS&CS Contractor Estimated Report Level(s): List Here

Program Office Estimated LOE*: \$XX,XXX.XX / Hours

**Note: for complex requests, it may be necessary to construct cost estimate by combining multiple report levels (e.g., working session for concept; initial draft; final report)*

Report Level Definitions

Level 1 – Basic Complexity

Level 2 – Intermediate Complexity

Level 3 – High Complexity

Notes:

List Here



4. TS&CS COR APPROVAL

Email all approvals to:

- Sylvester Smith: sylvestser.smith@gsa.gov
- (b) (6) jpidev.com
- (b) (6) jpidev.com

TS&CS COR: Sylvester Smith
Date Reviewed: MM/DD/YYYY

Approved for Production? ☐ Yes ☐ No

Appropriate Task Support Area:

☐ **Program Management Support**

Deliverable Name: Full Name of Report

☐ **Technical SME White Papers**

Report Levels: List Here

**Note: for complex requests, it may be necessary to construct cost estimate by combining multiple report levels (e.g., working session for concept; initial draft; final report)*

☐ **Technical Requirements Development, Reports, and Webpage Updates**

Development Type: List Here

☐ **Service and User Guides**

Guide Type: List Here

Task Area Funding Available: ☐ Yes ☐ No

Approved Request Description:

List Here

Notification Email Sent: ☐ Yes ☐ No

Notes (Schedule, Resources, etc.):

List Here

THE FUTURE OF CYBER ENABLED FINANCIAL CRIME:

*New Crimes, New Criminals,
and Economic Warfare*



A Threatcasting Lab Report



THE FUTURE OF CYBER ENABLED FINANCIAL CRIME:

*New Crimes, New Criminals,
and Economic Warfare*



Analysts:

Brian David Johnson - ASU
LTC Jason C. Brown - ACI/USMA
Josh Massad - Deloitte
Christopher Owens - USSS

The views expressed herein are those of the authors and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

The Threatcasting Lab is supported by



This project was supported by US Army Grant No. W911NF-20-1-0330.



ASU THREATCASTING LAB

Brian David Johnson	Director
Cyndi Coon	Chief of Staff
Ana Abasta	Coordinator
MDX Arts	Report Editor
MORR Design	Layout/Design



Arizona State University Threatcasting Lab

The Threatcasting Lab at Arizona State University serves as the premier resource for strategic insight, teaching materials, and exceptional subject matter expertise on Threatcasting. By using its approach, experts from multiple disciplines envision possible threats ten years into the future. The lab provides a wide range of organizations with actionable models to comprehend these possible futures as a means to identify, track, disrupt, mitigate, and recover from the possible futures as well. Its reports, programming, and materials bridge gaps, and prompt information exchange and learning across the military, academia, industrial, and governmental communities.



TABLE OF CONTENTS

EXECUTIVE OVERVIEW	10
Threats	10
Actions to be Taken	10
FORWARD	12
INTRODUCTION	14
BACKGROUND	16
Financial Crime Frameworks	16
Historical Context: The Dutch East India Company	20
Cyber Enabled Financial Crime	22
Societal Changes	23
FINDINGS	28
New Financial Crime(s)	28
The Effects of CEFCs on Vulnerable Communities	32
New Crime(s)	33
Economic Warfare	36
The Importance of Understanding Trust	38
Ladder to chaos	39
CEFC Conditional State and the	
Pre-Crime Paradox	40
Threat Outlier - An Additional Threat Area of Interest	44
INDICATORS (FLAGS)	46
Flags Definition	46
General CEFC Trends	46
Conditions	48
ACTIONS TO BE TAKEN (GATES)	50
Gates Definition	50
General Actions to be Taken	50
Actions specific to Federal Law Enforcement	55
FURTHER READING	56
APPENDIX A: SUBJECT MATTER EXPERT INTERVIEW TRANSCRIPTS	58





EXECUTIVE OVERVIEW

Research Question:

What will the future of cyber-enabled financial crime, perpetrated by either criminals or nation states, look like 10 years from now?

In the coming decade, those who engage in cyber-enabled financial crimes (CEFC) will take advantage of a collection of technologies and adjacent practices – creating new classes of crimes, conditions, and adversary vectors. There are numerous technologies at the forefront of societal evolution, including cryptocurrency, artificial intelligence, 5G, physical and digital autonomous systems, the Internet of Things (IoT), Smart Cities, biometric identity, space-based systems, and quantum computing. The combination of changes in these technologies and in society are likely to also include an over-reliance on digital devices, digital payments, monopolized smart systems, and broader technology dependencies. In addition, the nature of financial crimes is expected to change in that they will initially target vulnerable communities, consumers, companies, and cyber computer systems. Furthermore, financial crimes will increasingly be used to enable more advanced and egregious economic warfare opportunities for adversarial nations and nation-state proxies.

THREATS

- New Financial Crime(s) - Small target/

scale crimes by individuals and organizations for financial gain.

- Economic Warfare - Large scale economic warfare attacks by nation-states and their proxies to destabilize economies and erode trust.
- A Ladder to Chaos - A ladder from small to large targets wherein financial crimes mask a broader nation-state attack.
- CEFC Conditional State - A conditional state with a vacuum for criminals to expand “new crime” and for nation states to wage geopolitical, economic warfare.

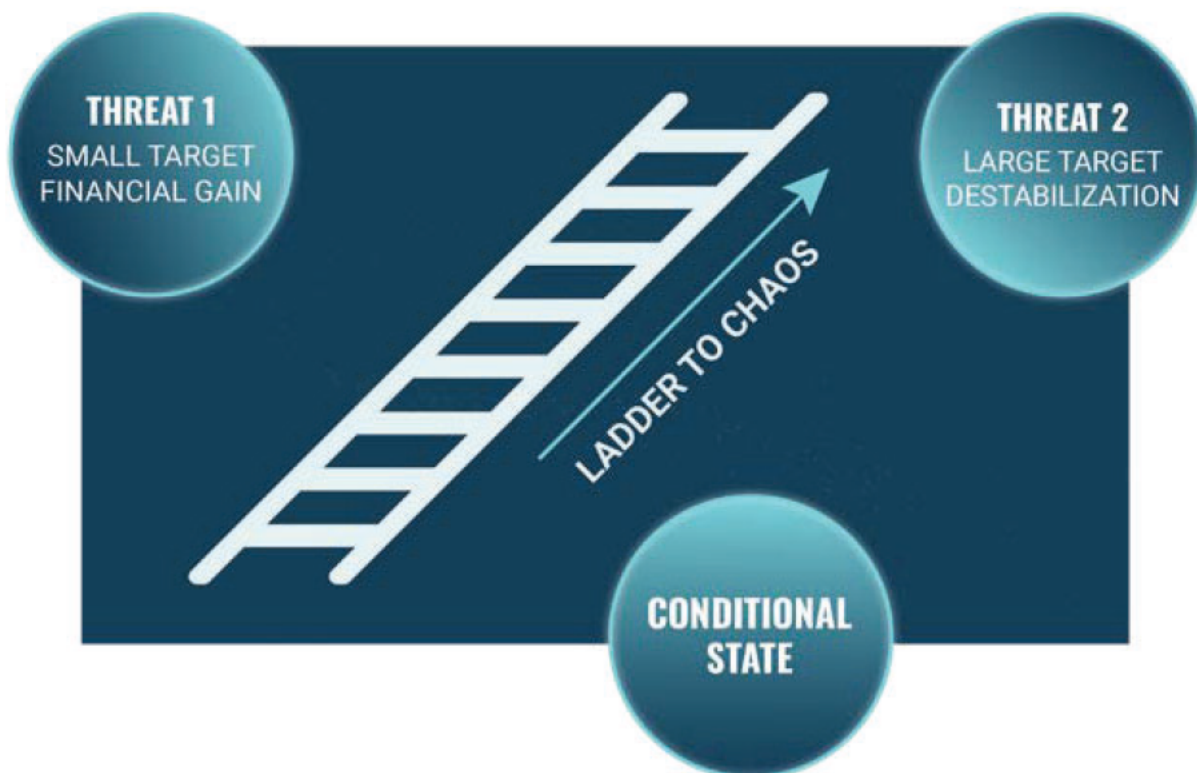
ACTIONS TO BE TAKEN

To disrupt and mitigate these threats, Federal Law Enforcement organizations should consider:

- Aligning their functional definition of CEFC technology and adjacent practices. The definition should address the differences between traditional financial crime and “new crime” that includes the increased impact of speed, scope, and scale of CEFC to federal law enforcement.
- Building a plan to empower, protect, and engage vulnerable communities (including consumers, companies, and computer systems) through lawful

monitoring systems that take into account the importance of identity, confidentiality, integrity, and availability.

- Developing a plan for tracking and monitoring emergent CEFC through sharing best practices across federal and local law enforcement, and the U.S. Department of Defense (DoD).
- Determining how to identify what is behind instances of CEFC, in order to unmask a potentially linked broader nation-state attack.
- Developing processes to pass the identification and intelligence of a CEFC from law enforcement to the DoD when jurisdictionally appropriate.
- Further exploring CEFC's pre-crime conditional state with indicators to watch out for and actions to take. Precedents exist for this shift, from a single criminal focus to conditional indicators, such as natural disasters and mass migration.
- Treating cryptocurrencies like real property.





FORWARD

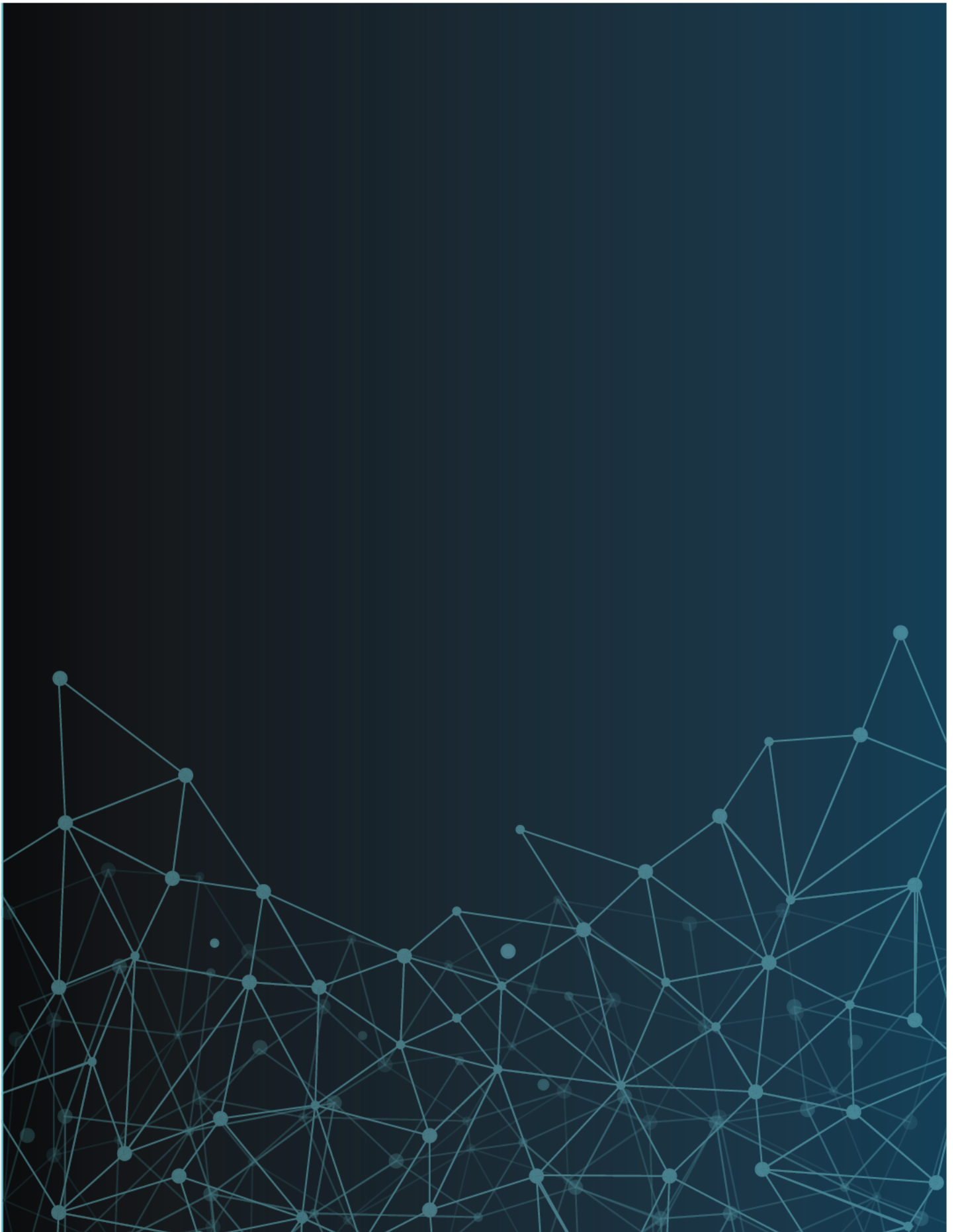
I am pleased to introduce this report jointly sponsored by the U.S. Secret Service and the U.S. Army Cyber Institute. It takes a rigorous, academic look at the insights of economists, bankers, strategists, futurists, and law enforcement professionals' consideration of potential future cyber-enabled financial crime scenarios.

Produced by Arizona State University's Threatcasting Lab, *The Future of Cyber-Enabled Crime: New Crimes, New Criminals, and Economic Warfare* will help policymakers and law enforcement personnel examine and prepare for the possible future consequences of complex, algorithm-driven financial systems, and their impact on U.S. and global economies.

As a federal agency responsible for investigating individuals and organizations engaged in crimes against the U.S. financial infrastructure, the Secret Service must continue to stay on the cutting edge of emerging financial and economic trends, including quantum computing and related encryption issues. Vulnerabilities in developing artificial intelligence and machine learning algorithms present new opportunities for cyber criminals determined to exploit financial systems for financial gain and economic disruption. As such, examining future threats is essential to readying policymakers, federal agencies, banking institutions, and the public to identify potential risk and respond accordingly.

I encourage all readers of this report to consider the vast scope of changes we have seen in recent years and imagine the broad range of innovation yet to come. As we advance technologically and socially, our adversaries will continue to evolve as well, using innovative methods to attack our systems and way of life. Adopting strategic foresight is essential to stay ahead of these threats and protect our financial infrastructure.

Gregory W. Try
Chief Strategy Officer
United States Secret Service





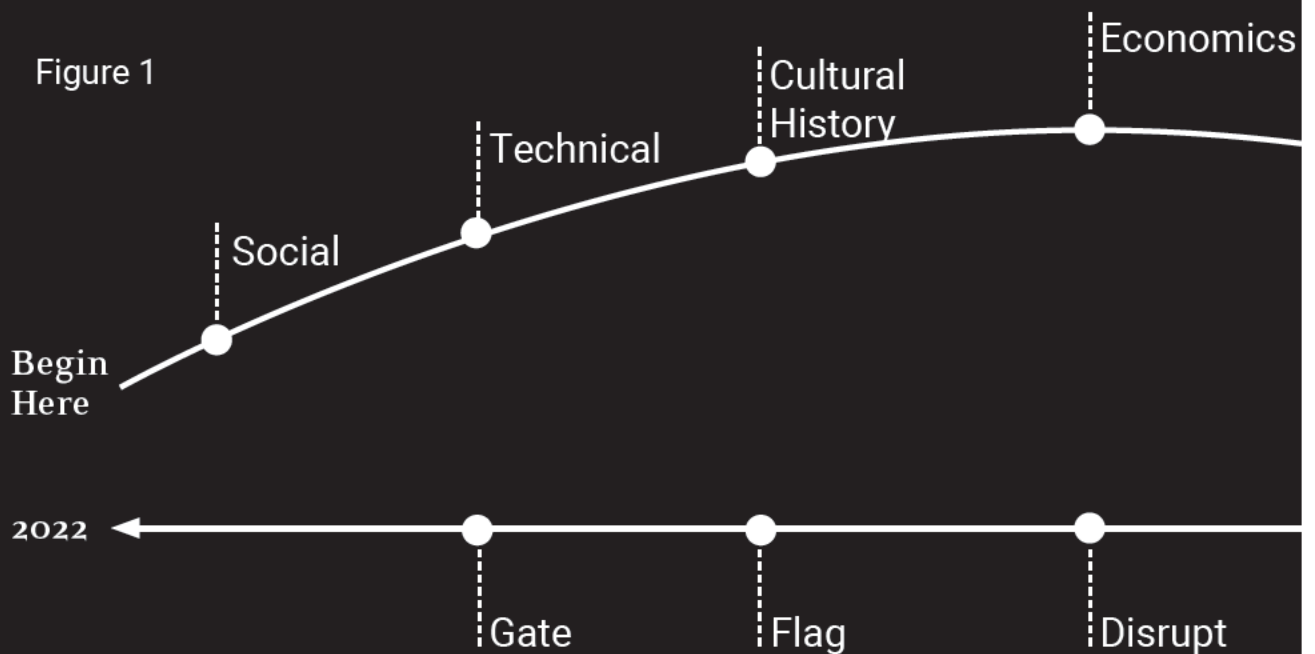
INTRODUCTION TO THREATCASTING

Threatcasting provides a systematic and transparent method to model a range of possible futures and threats in a complex and uncertain environment. Working with organizations via subject matter expert interviews, participatory workshops, and operationalization exercises, it provides decision-makers specific indicators that one or more of the futures or threats are

manifesting, with suggestions or possible actions that can be taken to disrupt the threat or pursue more desirable visions of the future.

Threatcasting is not designed to “predict” the future. Rather, the output of the methodology provides organizations and decision-makers a framework by which to

Figure 1



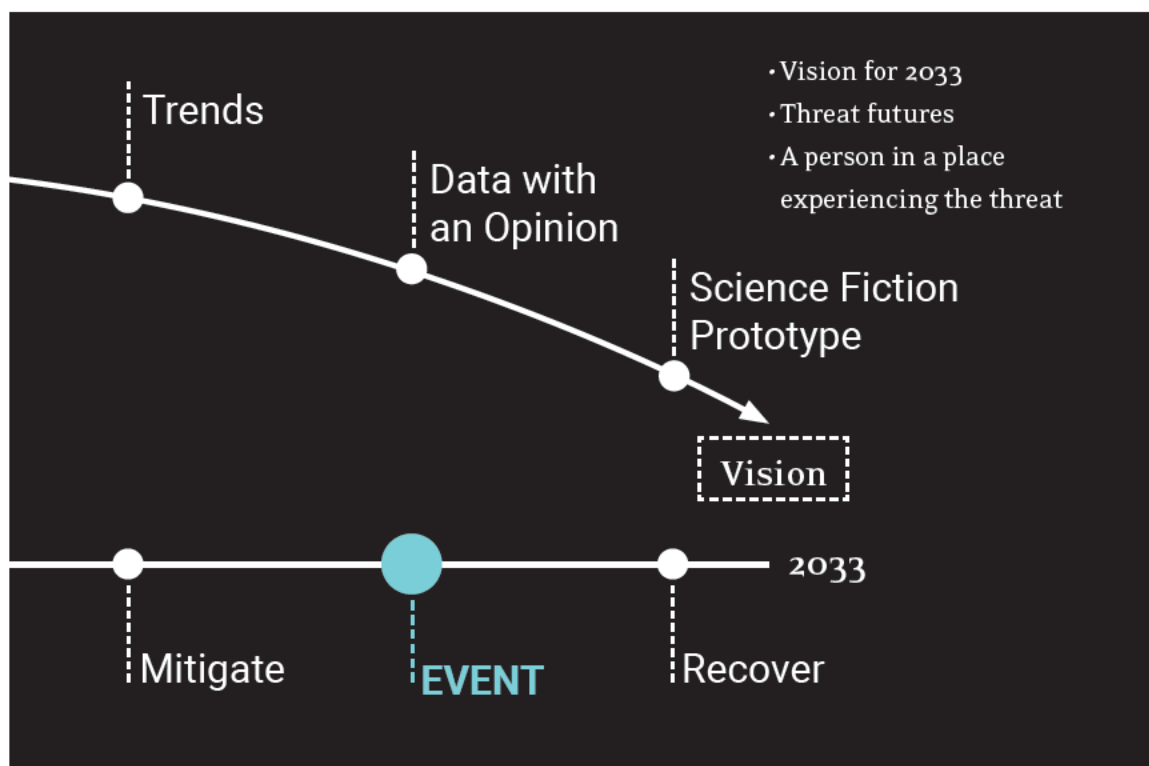
plan, prepare, and make decisions using their own perspectives on how the threats affect them.

Threatcasting often guards against strategic surprise. When a crisis occurs or an opportunity presents itself, a decision-maker or a leader is not caught off guard. Rather, their reply is: "We have talked about this before. We know where to start."

For this project, a cross-functional group of practitioners gathered for two days in November 2021, to create models of cyber-enabled threat futures. The outcomes of the session provided the initial framework for a set of possible threats, external indicators, and actions to be taken. Drawing upon research inputs from diverse data

and from subject matter expert interviews, participants synthesized the data into workbooks and then conducted three rounds of effects-based modeling.

In the Threatcasting sessions, participants generated numerous scenarios, each with a person, in a place, experiencing their own version of the threat. After the workshop concluded, analysts examined these scenarios to categorize and aggregate novel indicators of how the most plausible threats could materialize during the next decade and what the implications were for gatekeepers' standing in the way of the threats. While not predictive in nature, this process gives organizations a starting place to consider how CEFCs might affect them.





FINANCIAL CRIME FRAMEWORKS

This section covers how two existing crime frameworks were used to help make sense of the threat models developed in the Threatcasting workshop.

The first framework follows Peter Gottschalk's approach: This framework classifies financial crimes into families with similar characteristics.¹ Although Gottschalk's approach does not account for the emergence of digital currencies, his categories are useful for identifying the problem space. The Threatcasting lab adjusted some of Gottschalk's original classifications to better account for the future of CEFC.

- **FRAUD FAMILY**—These crimes include misrepresentation or deception with the intent of financial gain. This category encompasses traditional fraud crimes, including the ones closely aligned to digital currencies and crypto (e.g., identity theft, counterfeiting, Ponzi schemes, yield farming, liquidity farming, and rug pulls).
- **THEFT FAMILY**—These crimes involve taking money or things of value, but without the misrepresentation that

normally accompanies the fraud family of crimes. Examples include hacking and stealing private crypto keys, emptying an exchange, street-level mugging, and embezzlement.

- **MANIPULATION FAMILY**—This group of crimes adopts some of the more esoteric types of CEFC, such as influencing markets or prices, and developing cyber access for follow-on fraud or theft. Although developing cyber access may not first appear as a type of financial crime, the purpose behind most cyber intrusions is to steal data for resale, or for manipulating data for some future monetary gain. Causing an organization to react to an expensive cybersecurity threat is a form of manipulation, making these intrusions arguably a form of financial crime.
- **CORRUPTION FAMILY**—This category of crimes uses force, fear, and/or required payments for favorable treatment. Ransomware falls into this category, even though it might at first appear to better fit in the "theft" bucket. Ransomware is a type of corruption

offense because attackers often put a deadline into their demands, with the threat of some type of data spillage or permanent system lock-out if the demands are not met.

- **OTHER**—These crimes are adjacent to CEFC but are not necessarily “financial” crimes. The development of digital economies will bring with it crimes against society that create a social divide or a category of being “left behind”. While to many, this may seem like figurative social Darwinism (“keep up or die”), for the most socially vulnerable, “dying” could be quite literal. Consider electronic bank transfers for welfare recipients. Having all benefits

tied up in cumbersome, difficult to audit, and opaque systems puts people at real-life risk of starvation, disease, and death if they are unable to access their benefits and buy food.² This can be seen as an indicator of laddering up from small- to large-target crimes if these systems ever succumb to cyberattacks or other categories of financial crimes.



1 Gottschalk, *Categories of Financial Crime*, 441–58.

2 Team Obol 1 imagines Lisa, a low-income and food insecure single mother, whose access to government assistance is threatened as unattended algorithms continue to flag her account for trustworthiness problems caused by other algorithms. “The convergence of digital payments dominating the life of the average person and the over-reliance on AI to mete out services and civil punishments has left her destitute and hard-pressed to improve her situation.” See sidebar The Perils of Cyber Enabled Social Support on page 44

THE CRIME TRIANGLE



The second framework considered was the “The Crime Triangle”.³ Also known as a problem analysis triangle, this framework posits that three things need to occur simultaneously for a crime to happen. As shown in the image, the inner triangle consists of a target/victim, a place, and an offender. All three of these need to be present at the same time for a crime to occur. The outer layer of the triangle shows what is needed to mitigate the crime. A guardian protects the target, a handler monitors the offender, and a manager watches over the place. If just one section of the outer layer is present, the crime can be blocked.

³ The crime triangle (also known as problem analysis triangle) comes from one of the main theories of environmental criminology – the Routine Activity Theory, cited from Cohen and Felson, *Social Change and Crime Rate Trends : A Routine Activity Approach*, 588–608.



HISTORICAL CONTEXT: *The Dutch East India Company*

To explore the transition from traditional financial crime to CEFC, cultural historian Jamie Carrott researched other examples of the privatization of currency and levers of power.⁴ The Dutch East India Company (known scholarly as VOC⁵) and the English East India Company (EIC), give early examples of these types of transitions.

The following are some historical implications for the future of CEFC:

Piracy isn't just piracy.

Piracy is not just about theft. Piracy (officially "privateering") drove the global power shift in the early modern world. It allowed the relatively poor and scrappy English and Dutch to take down the Spanish and Portuguese empires, and was central to the success of both the Dutch and English East India Companies. It would not be an exaggeration to say that both companies were founded on silver and gold stolen from Spanish treasure fleets. Theft funded the whole enterprise, and it built upon itself. The VOC massacred indigenous populations in their quest to control the spice trade. The EIC⁶ turned mercenary, and

acted as a drug kingpin to build an empire that lasted into the middle of the 20th century, which ultimately drained significant wealth out of India.

When watching for change, look to the fringes.

Chipping away at the edges of a situation eventually undermines the dominant paradigm. Each individual act of rebellion or piracy may be survivable, but an empire can collapse under the cumulative weight of a thousand "cuts". What shifts the paradigm is not the piracy itself, but rather the undermining of the system – and blind faith in the system – that erodes "the dam" bit by bit, until the dam breaks and the river changes course.

When raw power is at risk, it is generally those on the edge of the power who are willing to break the rules and facilitate power shifts.

The medium is the message.

Money is not just about the raw power of exchange. An individual or group who issues, controls, and manipulates currency has substantial cultural power. The Portuguese established a monetary lingua franca or common language in the Asia trade. From the late 15th through 16th centuries, trade became normalized around a base value of the coin. Additionally, minting coins was highly symbolic. Specie, or money in the form of coins, was a literal representation of power—embodying their value in gold or silver. Rulers used coins to communicate power. Throughout the Mughal and European wars of the 18th century, one of the first things any new conqueror did was mint coins in their image. Digital currency, of course, lacks the physical symbolism or literal worth of a coin. What it does not lack, however, is the ability to communicate power. All forms of monetary exchange inherently contain a level of power.

Think flexibly.

Criminals are willing to break rules for personal influence, power, and profit. Often, they have little regard for countries, corporations, or other organizations. This requires organizations to think flexibly.

In the early modern world, power was less balanced, and the public vs. private dichotomy did not exist. Kings, Queens, and councils could delegate power in ways that today, most would find uncomfortable. An example of this is allowing a shareholder-owned company to develop and maintain an army, declare war, and/or print money.

The great successes of entities like the VOC and EIC were even more flexible. For instance, captains and governors often simply disobeyed orders and followed their own plans, which generally worked in the company's favor. This illustrates how the line between criminals and nation-states has been fluid.

One of the major findings described in this report is that seemingly small-scale crimes for personal gain can easily be scaled into a type of economic warfare, akin to the conflict that kings and presidents waged against other kingdoms or nation-states. The historical context of pirates and privateering reminds us that history may not repeat exactly as it did in the past, but it certainly informs how the future may look.

4 Carrott, *The Dutch East India Company and the Future of Currency*.

5 The English translation of *Vereenigde Oost-Indische Compagnie (VOC)* is the Dutch East India Company.

6 To expand, English East India Company entities like the VOC and EIC were more flexible. For instance, captains and governors often disobeyed orders and followed their own plans, which generally worked in the company's favor. The line between criminals and nation-states has historically been fluid.

CYBER ENABLED FINANCIAL CRIME

TECHNOLOGICAL DEFINITIONS WITH EXAMPLES

The following definitions were derived from analyst data and multiple subject matter expert (SME) interviews, including an economics professor at West Point and a blockchain analyst with U.S. Cyber Command. The definitions are not all-inclusive of the digital finance economy and cryptocurrency market, but are useful for understanding the findings of this report.

Blockchain Bridge - Allows for one party to exchange tokens of one crypto asset into tokens on another blockchain. As an example, imagine Alice has three Bitcoin (BTC) and wants to send five Ethereum (ETH) to Bob. BTC and ETH are on separate blockchains. A third person, Charlie agrees to take Alice's three BTC and sends the five ETH to Bob. Charlie acts as the bridge between Alice and Bob. Many crypto exchanges are centralized versions of a blockchain bridge. Bridges improve the ability for new traders to enter markets on other blockchains, but their centralized control is somewhat at odds with the benefit of decentralized networks.

Central Bank Digital Currency (CBDC) - Digital tokens issued by a country's central bank, attached to the country's fiat currency.⁷ Generally a fiat currency is any money made legal tender by a government. Often the national

government writes their own consensus protocol and ties it to taxes, so that users are forced to be compliant.

Consensus Protocol - The rules about how a blockchain verifies transactions on the network. Depending on the protocol, all (or some) of the computers on a network participate in verifying whether a transaction is valid.⁸ Some protocols reward the computers that finish the verification first, while others reward computers that do the most work.

Distributed Ledger - A decentralized database of transactions and records that are shared and updated by all members of the network. All participants are governed by the network's consensus protocol rather than by a central authority. Because all participants on a network have a copy of the ledger, once a transaction is written and shared, the record becomes immutable and auditable.⁹

Oracles - Computer programs that act as bridges between the real world and a blockchain. An oracle watches for certain conditions that a smart contract needs to execute. For instance, an oracle could monitor stock prices and when a specific stock reaches a set price that is written into the contract, the oracle signals the blockchain that the contract condition has been met and to execute a buy or sell order.¹⁰

Private Key - A series of numbers and letters that make up the key to unlock your assets on a blockchain or in a crypto wallet. The private key authenticates a user on a network. It is the single most critical piece of information a person needs to conduct transactions on a blockchain. For instance, if a user loses their private key, there is no way to access their assets on the blockchain. Similarly, if someone gains access to this key, they can make transactions with the original user's assets. The companion piece of information is one's public key, which is like an email address, so others know how to contact the person for transactions.

Seed Phrase - A string of 12 to 24 words that act as the master password for an individual's crypto wallet. The seed phrase generates private keys necessary to authenticate a user and their transactions on the blockchain network.¹¹ Safeguarding the seed phrase is essential to the security of the private key.

Smart Contract - Tiny pieces of computer code that carry out certain instructions and may be tied to the execution of another

linked contract. They are usually a form of "if...then" statements written in code and stored as a record on the blockchain.¹² When the "if" condition is met, the computers on the network run the "then" statement of the contract. Once the contract is executed and accepted by the blockchain, it becomes immutable. Malicious, malformed, or improper smart contracts can attack the network, usually for significant monetary loss to one party.¹³ Contract attacks are a growing area of concern for security specialists and financial crime investigators.

SOCIETAL CHANGES

The development and deployment of emerging technologies will not be the sole enabling factor for CEFC. As technologies mature, populations, markets, and industrial applications will utilize them to create new businesses and societal activities. The following are key societal changes enabled by technology that will create the environment for CEFCs.

7 Seth, *Central Bank Digital Currency (CBDC) Definition*.

8 Kramer, *What Are Consensus Protocols?*

9 Brakeville and Perepa, *Blockchain Basics: Introduction to Distributed Ledgers*.

10 Injective Labs, *What Is a Crypto Oracle?*

11 Coinbase, *What Is a Seed Phrase?*

12 Hussey, Matt, and Phillips, *What Are Smart Contracts and How Do They Work?*

13 Innocent, *Smart Contract Security: The Attacks and Solutions*.

Wealth and Investment - There are three things to consider as cryptocurrencies shift to become a larger portion of an individual's wealth.

First, the threat models produced in the workshop suggested that more people will use cryptocurrencies of various sources – in addition to Bitcoin, Ethereum, and other front-runner currencies. A larger percentage of individuals' net worth is expected to be tied to crypto, and much of it could be uninsured. Examples include retirement plans and college funds stored as crypto assets.

Second, corporations are likely to begin “dabbling” or investing small amounts of money in a variety of e-currencies and digital commodities as part of their long-term financial strategies. Corporations with sufficient reserve funds should be able to weather crypto market instabilities better

than individual investors, thereby giving corporations stronger control of crypto-involved wealth.

Third, there are a number of variables that have tremendous potential to expand the “digitally disadvantaged” class, including the unbanked. These include a lack of fiscal education and awareness at the individual consumer level, as well as rapid financial model shifts that are tied to increased investments in digital commodities. Although decentralized finance (DeFi) tools, such as cryptocurrencies and digital commodities should increase the availability of these markets to currently unbanked individuals, research doesn't yet address the extent to which this population will have access to DeFi tools. What is needed is an accompanying educational push by the federal government or the DeFi community.



Confidentiality, Integrity, Availability (CIA)

- In the world of information security, the CIA triad represents 1) Confidentiality – an individual's data is available only to him/her and other authorized viewers; 2) Integrity - an individual's data is true and has not been changed; and 3) Availability - an individual can access his/her data whenever s/he needs to. This triad is the foundation of trust in data and computing. The workshop's threat models indicated several ways in which this trust might be thwarted with the advancement of future CEFCs.

Early successful attacks on institutions that develop and support digital currencies and digital commodities could create a delay and reduce trust in the digital banking system. Cryptocurrency exchanges have recently lost billions of dollars in thefts and hacks,¹⁴ slowing the growth of crypto investment. Banks and financial institutions that are hacked are likely to similarly lower

the confidence in both the digital economy and federal government that are backing any plans for centrally supported, digital finance tools and markets.

It's also expected that a new market will be developed for third party actors who manage digital identity authentication tools and data integrity checks. With these authentication technologies, criminals could take advantage of advances in biometrics, digital passports, microchips and implants, tattoos, and/or DNA-based secure tokens. They, and the businesses that develop around them, will be under intense scrutiny from consumers who need the technologies to work as advertised and from regulators who will insist that privacy leaks are minimized. It's also projected that there will be a concurrent black market that will manipulate, counterfeit, or otherwise defeat digital identity authentication technologies.

¹⁴ Browne, *Criminals Have Made off with over \$10 Billion in 'DeFi' Scams and Thefts This Year.*



Digital Life - Another underlying condition in the future of CEFC is the inevitable reliance on digital devices. Society is expected to run wholly supported by the Internet of Things (IoT). The dilemma arises when something happens to disrupt electrical grids, cell phone towers, and/or portions of the internet that move IoT data. As the transition to digital-only services continues, artifacts such as land-line phones, brick-and-mortar banks, and even in-person medical appointments will be significantly reduced. This threatens the capability to recover from disruptive events.

Artificial Intelligence (AI) - It's difficult to discuss a digitally-supported life without understanding how AI technologies underpin it. Likely the only way to keep up with the speed, scope, and scale of CEFC is with a clear understanding of automation, or more precisely, the use of algorithms, AI, machine learning, and other technologies where humans are not making all the decisions. Future criminals will attempt to exploit victims at the individual level, using insights from their publicly available information (e.g., from social media platforms) or private information (e.g., their crypto wallet private key). Criminals are also likely to use AI and automated tools to climb the ladder into wide-spread economic crime and even into state-sponsored economic warfare. However, AI is also expected to be used as a defense against digital criminals, even to the point of algorithms battling each other. This means that while AI can improve public trust in digital payments by ensuring their

confidentiality, integrity, and availability, it can also create vulnerable communities. The complexity and proprietary nature of many AI systems often prevents human interaction until it is too late to mitigate unintended harm.

Regulation - Over the next decade, a continued struggle is expected between regulation and decentralization. The technologies that make up cryptocurrencies and the crypto market were originally intended to be decentralized and subject to control of the community consensus. At the same time, law enforcement agencies are rightly focused on stopping the rampant money laundering, fraud, theft, and other illicit activities that occur due to the decentralized nature of crypto-based financial crimes. While the law often lags behind criminal innovation, over time, diverse CEFC cases will provide regulators with a better understanding on how CEFC works and what legal authorities will best equip law enforcement to fight it.

Regulation to counteract CEFCs might take advantage of three different types of efforts. The first type of regulation would be to hold platforms responsible for the activities of their users. A second helpful regulation would be for government entities to provide guidance and boundaries for the private insurance industry to make sure individuals have recourse for recovering lost money. A third regulation would be to combine forces with cross-border agencies, whether through international criminal investigations (INTERPOL, EUROPOL) or

through industry-wide standard setting at the United Nations, International Monetary Fund, and/or the World Bank.

New Iterations of Old Schemes -

The future of CEFCs is projected to see criminals trying to adapt old schemes with new technologies. They will likely take advantage of the fact that there is a gap between when a new technology appears and when law enforcement and regulators can act to understand, investigate, regulate, and minimize the opportunities for criminal gain. It's expected that known grift, con, fraud, and theft techniques will be applied to digital banking and crypto currencies. Most of the criminals' successes are likely to come from exploiting the unaware, especially by using those schemes that promise a mirage of success, as individuals will not know where to look to verify or confirm whether a scheme is valid or not. Some methods will immediately evolve as regulation and law enforcement catch up to the criminal activity more quickly than anticipated. Other possibilities include adaptations of crypto fraud as a service, like the evolution of denial-of-service attacks and ransomware attacks as services-for-hire on the dark web.





NEW FINANCIAL CRIME(S)

CEFCs are expected to first appear as acts against vulnerable consumers, companies, communities, and/or computer systems and networks (VCs).

Additionally, the CEFC environment will give rise to new forms of financial crime that do not fit in existing crime frameworks. These “New Crime(s)” will challenge federal and local law enforcement’s existing understanding of crime prevention, detection, and prosecution.

Over the next decade, the emergence of New Crime(s) will first be seen in the VCs. VCs will not be as ready or equipped to respond effectively, thus making the population even more vulnerable.

SMALL TARGET/SCALE CRIMES

by criminals and organizations
for financial gain

THREAT 1
SMALL TARGET
FINANCIAL GAIN

LADDER TO CHAOS

CONSUMERS:

A broad range of the U.S. public can fall into the “vulnerable” category. Essentially, a population is considered vulnerable because they lack resources to address criminal behavior (e.g., information, capital, social safety net, experience).

- Example Vulnerable Consumers:
 - Retired veterans,¹⁵
 - Elderly,¹⁶
 - Retirees, and
 - Youth and young adopters.¹⁷
- Vulnerable consumers have specific areas where they are affected or susceptible to CEFCs, including:
 - Personal data, often referred to as personally identifiable information (PII),
 - Personal devices that act as a 'gateway' for cyber exploitation and additional theft,
 - Individual financial information,
 - Financial portfolios,
 - An individual's entire digital, financial, and societal presence, and
 - Digital currencies.

15 Retired veteran scenario: Team Buckzoid 1 imagines Josh, a retired and disabled military veteran experiencing AI-enabled fraud through an online veteran support group. The AI digitally “resurrects” dead people's online profiles and procedurally generates life updates. Josh's support group is filled with these AI ghosts, and it pulls him into a multi-level marketing scheme converting his money into Bitcoin, of which he understands very little.

16 Elder scenario: Team Dhama 2 imagines Auntie Irma, a pensioner living in Florida who is trying to catch up on her retirement accounts after the 2029 European Union Financial Collapse took nearly everything. Her desperation to reestablish a safety net makes her look past the warning signs of yet another online crypto investment site that is not fully vetted. She loses her safety net – again.

16 Youth and young adopter scenario: Team Drachma 2 imagines Jane, a professional in her early 20's who lives in Washington, DC. Jane invests in an NFT (non-fungible token) artwork consortium (like a timeshare) and then “rents” her portion of the NFT access to other people on her social media platforms. The NFT consortium is owned by a foreign social media site and since Jane didn't carefully read her contract, her “rent” income legally belongs to the consortium, and therefore to the foreign media site.

COMPANIES:

Vulnerable Companies provide a different attack surface for CEFC.

- **Small Businesses:** Typically, vulnerable companies are small businesses without the resources to address criminal behavior (e.g., IT staff, security knowledge, up to date systems). Small businesses might be overwhelmed by legislation, insurance agencies, or previous lawsuits and attempt to take shortcuts to meet their profit goals.
- **Large Enterprises:** Some vulnerable companies can be large national or international organizations. Their vulnerability stems not from a lack of resources but by their size and scale, leaving blind spots and holes in their security posture. Additionally, these large organizations may have legacy technical systems that have not been updated or replaced because they have escaped the notice of their IT security department.

COMMUNITIES:

"Communities which include, but are not limited to, women, racial or ethnic groups, low-income individuals and families, individuals who are incarcerated and those who have been incarcerated, individuals with disabilities, individuals with mental health conditions, children, youth and young adults, seniors, immigrants and refugees, individuals who are Limited English Proficient (LEP), and lesbian, gay, bisexual, transgender, queer and questioning (LGBTQQ) communities, or combinations of these populations." ¹⁸

- **Example Vulnerable Communities:**
 - Underserved populations,
 - Unbanked populations,
 - People at different age groups with varying understanding of digital economy threats and opportunities, and
 - People subject to authoritarian regimes enacting CBDC controls.¹⁹

COMPUTER SYSTEMS AND NETWORKS:

Vulnerable computer systems and networks can also be categorized as “vulnerable companies”. Simply by using computers and attached networks, organizations themselves are vulnerable to attacks. The organizations may be businesses in private industry, but can also include governments, non-profits, and/or advocacy groups.

- Examples of vulnerabilities of computer systems and networks are:
 - Small companies with small security budgets, and
 - Large organizations with legacy systems that are not incentivized to update or replace for financial reasons.
- How they are vulnerable:
 - The “cyber world” allows for a quantity of small thefts instead of targeting large thefts.²⁰
 - Individuals who are vulnerable may rely on a single device, which leaves no redundancy or back-up system to access information.
 - Personal investment portfolios can be exposed to attack and theft when not completely secured.
 - An individual's lack of wealth may motivate them to take more risks.
 - Individual 'trust' relies on the amount of knowledge and time IT teams can invest in security.

18 Law Insider, *Vulnerable Communities Definition*.

19 People subject to authoritarian regimes enacting CBDC controls scenario: Team Talton 2 imagines how Olayinka Adebayo, a respected investment banker from Lagos, Nigeria, is watching his country become consumed and dominated by Chinese politics. Because Nigeria runs the only accepted African digital currency backed by a central government, this effectively gives Chinese businesses de facto control over much of Nigeria's, and by extension, Africa's economy.

20 The “cyber world” allows for a quantity of small thefts instead of targeting large thefts scenario: Team Drachma 1 imagines Sam, a hardware store owner in Chicago who combines his personal and business funds to access high-speed trading algorithms. Not only does Sam make bad business decisions, but he also discovers that the trading company he is using has signed him up through an algorithmically-based phishing scheme that looks for small business owners seeking loans. The illegal trading company is subsequently hacked and all his personal and customer information is leaked online.

THE EFFECTS OF CEFCS ON VULNERABLE COMMUNITIES

The magnitude of the effect on a victim usually determines whether someone will go after a bad actor or not. Often "the juice isn't worth the squeeze" for financial companies or even for individuals with a modicum of security. If small amounts of money are taken, and it is difficult, frustrating, and/or time consuming to try to get the money back or to get retribution, victims may just move on. Adversaries have

historically tried to get as much out of one victim as they can because of the effort and time needed to respond by isolating and targeting them effectively. But with countless vulnerable individuals now easily accessible through cyberspace, the time needed to respond rarely exists. Therefore, a bad actor can achieve greater results without triggering a response.



NEW CRIME(S)

Much of the emerging criminal activity is projected to fall under existing definitions of financial crime, yet the CEFC landscape will allow for “new crimes” to emerge. These new crimes are anticipated to arise from the combination of technologies and societal practices that materialize over the next decade.

It is helpful to think of this activity as “new” because it falls outside of the traditional definitions of financial crime. The nature of this difference, shifting from previous definitions to new definitions, will be enabled by the emerging CEFC environment – providing variations of traditional crimes as well as new classifications. Here is a recent example of a new crime today, how it has become mainstream, and which points to the potential continued evolution of criminal behavior:

A (recent) operation coordinated by INTERPOL, codenamed HAECHI-II, saw police arrest more than 1,000 individuals and intercept a total of nearly \$27 million of illicit funds, underlining the global threat of cyber-enabled financial crime.

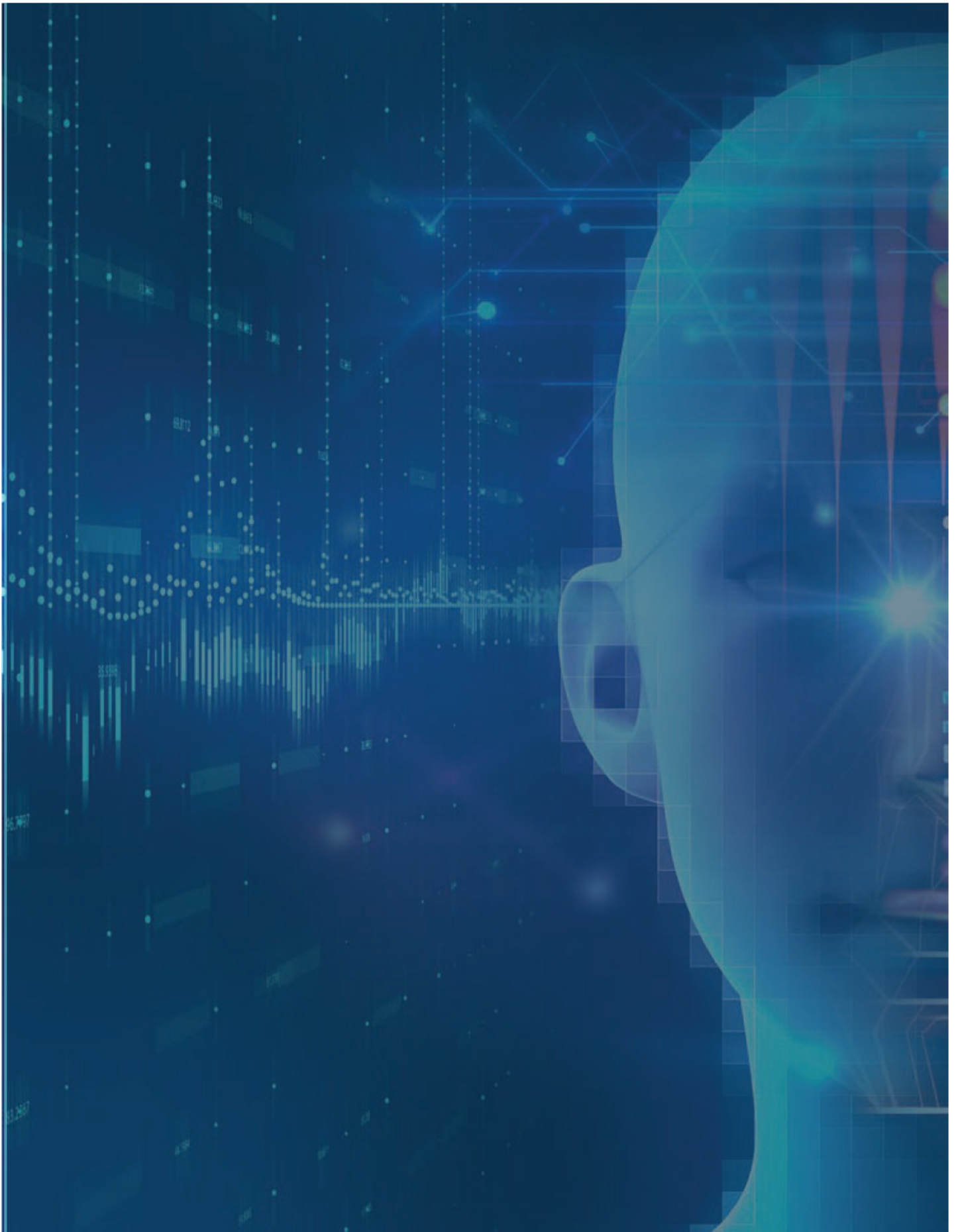
In total, the operation resulted in the arrest of 1,003 individuals and allowed investigators to close 1,660 cases. In addition, 2,350 bank accounts linked to the illicit proceeds of online financial crime were blocked. More than 50 INTERPOL notices were published based on information relating to Operation HAECHI-II, and 10 new criminal modus operandi were identified.

Far from the common notion of online fraud as a relatively low-level and low stakes type of criminality, the results of Operation HAECHI-II show that transnational organized crime groups have been using the Internet to extract millions from their victims before funneling the illicit cash to bank accounts across the globe.²¹

²¹ Homeland Security Today, *Massive Cyber-Enabled Financial Crime Crackdown Included ‘Squid Game’ Trojan Horse*.

The following are examples and indicators of the New Crimes explored during the Threatcasting workshop:

- **Impact** - The CEFC environment will enable bad actors to have a larger impact in the future, because they have the capacity to act as a multiplier. Having a multiplier effect enables crimes to spread quickly among victims and across the globe. This increased impact will also make the CEFC environment attractive to nation-states and their proxies, as a place to have a wider destabilizing effect.
- **Speed, Scope, and Scale** - The CEFC environment will provide bad actors with efficiencies in speed, scope, and scale. These will accelerate a crime's impact and create the capacity to build upon original crimes to create new opportunities and New Crimes.
- **Cultivated Synthetic Identities At Scale** – Traditionally, hijacking or impersonating a person's identity has been a cornerstone of financial crime. However, the CEFC environment, specifically the use of biometrics and AI, is expected to provide attackers the ability to create custom-built synthetic identities at scale. These identities will be “grown” or “groomed” for specific purposes to evade detection for long periods of time or possibly all together.
- **Synthetic Identities in the Physical World** - When synthetic identities are connected to their cultivated biometrics and linked to the growing network of IoT (e.g., in the case of carrying out financial transactions), the synthetics will start to have an observable presence in the physical world. Their biometric and IoT presence will make them even harder to detect when digitally monitored and verified.





ECONOMIC WARFARE

THREAT 2 LARGE TARGET DESTABILIZATION

An outcome of CEFCs is projected to be large target, economic warfare attacks by nation-states and their proxies to destabilize economies and erode trust.

The economic warfare threat shifts the target of the criminal activity and the intent of the crime to destabilization.

Threatcasting definitions of the manipulation and corruption families of financial crimes are used as the basis for understanding economic warfare. The manipulation family includes those who attempt to influence markets and prices, and further encompasses cyber-attacks for follow-on fraud and theft operations. Corruption crimes are those that invoke force, fear, or payments for favorable treatment, including ransomware attacks.

These families of financial crimes share strong dependencies on rapidly evolving technologies, crypto-assets, poor or absent regulation and oversight. In addition, they can happen at both the individual and aggregate level. Disruption – even temporary – is the goal, and sowing distrust or chaos can be as valuable as actual financial theft.

Economic warfare is a large umbrella term that legal experts traditionally describe as “economic and financial hostilities as activities that fall below the threshold of warfare.”²² This can also be described as “gray zone warfare” or actions taken by both state and non-state actors, just short of a kinetic conflict. Threatcasting Lab findings revealed a growing concern that financial hostilities, either purposefully enacted by adversarial nations, or accidentally aggregated through targeted small crime activities, should be considered in a different light.

Recent economic problems in America and Europe illustrate how connected individual financial institutions are to both the private consumer and national economies. National and global financial interdependencies have resulted in systemic risks, often framed by policymakers as “too big to fail,” “too connected to fail,” and “too fast to save”.²³ This means that small concerns at one end of the system can lead to catastrophic economic consequences at the other end.²⁴

The Financial Stability Board, an international body that monitors and



makes recommendations about the global financial system, assesses that as crypto assets become adopted at more financial institutions, their linkages to the broader financial system will be more profound. This means that the ladder linking of small and large target crimes allows for stronger scaling up of the impacts of CEFCs. Attacks against individual consumers will have an aggregated impact on crypto-backed economies. Similarly, as financial institutions add crypto assets to their portfolios, they assume risks as if they were an individual consumer. Blockchain transactions do not recognize whether the parties involved are a “Mr. Smith” or a large financial institution.

The Financial Stability Board assesses that “If current trends continue, and are absent effective regulation and supervision, financial stability risks may emerge as crypto-assets become increasingly interconnected with the wider financial system. This is especially the case in emerging market and developing economies (EMDEs) where crypto-assets may in some situations replace the domestic currency, or offer opportunities to circumvent exchange restrictions, and capital account management measures.”²⁵

Economic destabilization might occur in numerous areas, including:

- 
- National economies,
 - National or international businesses,
 - Microtargeting campaigns,
 - Mass identity theft,
 - Transnational financial crime rings,
 - Business databases,
 - Business supply chains,
 - Online shopping/retail businesses,
 - Energy grids or supply chains,
 - Loss of faith in financial institutions,
 - Loss of faith in federal currency,
 - Stock markets,
 - Global aid relief, and
 - Nation-state economic and currency competition.

With a broader goal, perpetrators of financial crimes shift from criminals and criminal organizations to nation-state actors or their criminal proxies. Because of this shift, the classification of the crimes moves from financial crime to economic warfare.

²² Lin, *Financial Weapons of War*, 1377–1440.

²³ Ibid.

²⁴ The “Flash Crash” of May 6, 2010 witnessed unprecedented market instability and loss of market value estimated at \$1 trillion in less than thirty minutes. See Bowley, *Lone Sale of \$4.1 Billion in Contracts Led to ‘Flash Crash’ in May*.

²⁵ Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-Assets*.

THE IMPORTANCE OF UNDERSTANDING TRUST

The idea of trust, either explicit or implied, was present throughout the workshop. Participants often built scenarios that included mitigation of crime through legal authorities. Participants' trust in law enforcement would sufficiently put an end to an imagined crime scheme they developed in the workshop. Their imagination built complex and theoretical future crimes. But ultimately, when backcasting the scenarios, participants often relied upon traditional law enforcement, empowered by new authorities or technology, as the primary cure to crimes.

The public also relies on the safety of banking systems and trusts that they can be protected by them. Likewise, they place their trust in law enforcement to stop crime when banking systems fail to offer protection. Bad actors display trust in another form. They trust that electronic banking networks are built upon systems that can be exploited for financial gain. Lastly, law enforcement relies upon legal authorities to provide the ability to investigate, mitigate, and levee punishment against criminal behaviors.



LADDER TO CHAOS

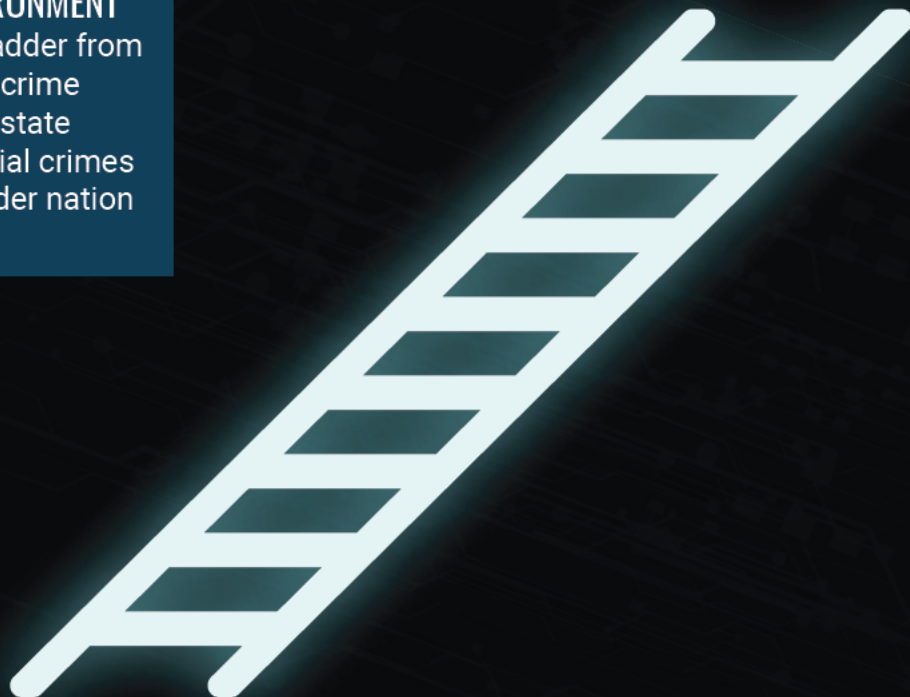
A criminal activity that first appeared in the workshop with the goal of financial gain from VCs, highlighted a unique threat space. This first appearance was referred to as Threat 1. The impact, speed, scope, and scale of the attacks began to show that this criminal attack was masking a larger economic warfare assault, which was labeled Threat 2.

As the criminal activity escalated, a Ladder to Chaos was identified as Threat 3, affecting more people with the goal of destabilizing organizations, markets, and countries.

Effects Trigger

It may be possible to observe when personal financial crimes are masking a larger nation-state attack. This can be identified through the nature and effects of the attack. When the volume of the personal financial crime reaches a certain level (i.e., a high volume of attacks in a specific place or industry), the “effect” of the attack also shifts. In other words, the goal of the attack is assessed to move from financial gain to larger nation-state destabilization. The volume of attacks and the eventual broader destabilizing effect becomes a potential trigger that can identify the nature of the attack.

THE CEFC ENVIRONMENT
will provide a ladder from
small financial crime
to large nation-state
targets. Financial crimes
will mask broader nation
state attacks.



CEFC CONDITIONAL STATE AND THE PRE-CRIME PARADOX

CEFCs will create a conditional state with a vacuum for criminals to expand New Crime and for nation states to wage geopolitical economic warfare. This will necessitate a greater focus on the underlying conditions, rather than on the perpetrator or singular crime.

Pre-Crime Precedents

The notion of “pre-crime” can stimulate science fiction visions of the future, like those portrayed in the 2002 Steven Spielberg thriller, “Minority Report”. Based on the Philip K. Dick book of the same name, the story centers around an oppressive police state that uses “precogs” or humans with the ability to foresee possible future crimes, prompting arrests

of suspects before they have committed the actual crime.

However, in reality, “pre-crime” is an emerging study of societal and natural conditions, which has the potential to give rise to a higher frequency of specific sets of crimes perpetrated on specific sets of people.

Pre-crime laws and practices can be organized into the following four categories that fall within the definition of ‘substantive coercive state intervention targeted at non-imminent crimes’²⁶:

- Pre-emptive criminal classification imposed on young offenders,
- Crimes of association and encouragement,
- Detention or restrictions on the basis of capability, and
- Interventions based on suspicion of intent.

“VACUUM FOR BAD ACTORS”

Conditional State that creates a space for criminals playing the long game of Geopolitical conflict.



CONDITIONAL
STATE

Another example of pre-crime activities can be seen in Norway and the exploration of the implications of mass migration on crime rates. Norway and Europe were concerned about an increase in migrants and follow-on effects of open borders. Concerns about increased crime, reduced public safety, and a lack of identity checks led to more control measures within the Intra-Schengen program. Border control practices in Central and Western Europe become more protective and securitized.²⁷ Norwegian police updated their police intelligence doctrine and launched Operation Migrant as the very first national intelligence project. The idea of a crisis “encouraged worst-case scenario thinking that generated suspicion and unease, especially among politicians, about potential criminal repercussions of this increase in migration.”²⁸

The Pre-Crime Paradox

Pre-Crime vs. Post-Crime

For law enforcement, this pre-crime type of thinking could be considered counter-intuitive to traditional approaches that address crime reactively. A recent example of the emerging exploration of pre-crime as opposed to post-crime is illustrated

by Australia's response to the 9/11 terror attacks.

“Prevention in Australia’s domestic legal response to terror has ushered in a host of ‘pre-crime’ measures that permit the state to intervene and restrain an individual on the basis of an anticipated future harm, rather than past wrongdoing (Zedner, 2007a: 259). Prevention by liberty restraint is a feature of many anti-terror initiatives, most notably control orders and preparatory offences (Divs 101, 104, Criminal Code Act 1995 (Cth) ‘Criminal Code’). These measures deviate from the traditional retrospective and ‘post-crime’ orientation of the criminal justice system, where the state reacts and responds to harm by prosecuting and punishing criminal acts on the basis of evidence gathered about past events (Roach, 2010; Zedner, 2007a: 259, 2009: 73). ‘Pre-crime’ measures are predictive and rely upon intelligence ‘about future threats to security’ gathered through surveillance practices and ‘pre-crime’ policing (Roach, 2010: 52; Walker, 2011: 56).”²⁹

26 Gobeil and Justin. *Review of McCulloch, Jude, and Dean Wilson and Pre-Crime: Pre-Emption, Precaution, and the Future. Surveillance and Society.*

27 Jansen, *Pre-crime and Policing of Migrants: Anticipatory Action Meets Management of Concerns*, 90 –10.

28 Ibid.

29 Tulich, *Prevention and Pre-Emption in Australia's Domestic Anti-Terrorism Legislation*, 52.

A NEW LENS THROUGH WHICH TO VIEW CRIME

The following compares and contrasts two differing approaches to crime – “Static” and “Evolving.” The Static approach sees crime as finite, meaning that crime will come to an end if addressed. The Evolving approach, however, employs a different lens through which to view crime. It sees crime as ongoing and constantly changing, as long as there are opportunities.

This Static approach typifies the traditional law enforcement method and mental model for understanding how to combat traditional financial crime. Historically, law enforcement uses the categories of victim, perpetrator, investigation, and prosecution. Laws, law enforcement policies, and insurance approaches to managing financial crimes are pinned to this categorical model. However, the future of CEFC requires a new mental model. Law enforcement needs to update the lens through which it sees crime as Evolving in the CEFC landscape.

For small crimes, the Static approach usually makes sense. There is a victim,

a criminal, and a set of activities by lawmakers to investigate and prosecute. In this case, the victim has a sense of justice. But this approach only works for the Fraud and Theft categories of crime.

The Evolving approach requires a different mindset. The speed, scope, and scale of future crimes has the potential to evolve into whole-of-government, economic warfare. Many of the same indicators as small target crimes are expected to be present, but with a wholly different intent behind them, and the responses to them cannot be the sole responsibility of law enforcement agencies.



STATIC

- Federal Agencies use of terms and defined goals
- "Impose consequences"
- "Change behavior"
- "Investigate violations"
- "Increase voluntary compliance" with tax laws IRS
- Disinformation/propaganda
- Prosecution of individuals as a goal
- Accountability to foreign bad actor
- Accountability or sanctions against foreign nation
- Regulations and standards put in place by law enforcement
- "Put an end to crime" as a goal
- Same tactics with new technologies
- Social net replaced by technology

EVOLVING

- White collar crime motivation "to obtain or avoid losing money, property, or services or to secure a personal or business advantage"
- Frequent use of "investigate" by federal law enforcement agencies
- Small operations intended to determine weaknesses and vulnerabilities
- Disruption, distrust, and chaos of economic security rather than theft
- Negative economic influences
- Loss of wealth growth, not the same as theft of wealth
- Manipulation of digital currency markets
- Dynamic nature of digital crime
- There is no 'bad op' when something is learned or discovered
- Organized criminal organizations persistence beyond the capture of one leader
- "Do even better next time" as a goal
- Tier 1 countries resistance to change (or slow change) allows enemies to attack the same defenses repeatedly
- A sense of security in believing you know someone as well as believing you know the technology. As always, belief in security is the thief's best friend.

THREAT OUTLIER - AN ADDITIONAL THREAT AREA OF INTEREST

The Perils of Cyber-Enabled Social Support

There is one interesting outlier that does not explicitly answer the Threatcasting research question, but analysts recognized it as a critical nexus of financial insecurity. It occurs when cyber-enabled social support fails. As automation technologies converge with ubiquitous digital financial systems and social support systems (e.g., welfare, prescription drug payments, child support), there is a possibility that vulnerable populations will be locked out of their support system(s) and their vulnerabilities will be further exacerbated. This could be considered a type of financial crime that the government inadvertently commits as its leadership places more trust on automated systems.

Threat Overview

In the CEFC environment, public benefits and payday loans are digitally issued and at risk of hacking, confiscation, and/or becoming inaccessible due to internet connectivity.

Below is a hypothetical case study that illustrates the effects of this threat.

Lisa is a low-income and food-insecure, single mother of an only child who lives in deindustrialized Gary, Indiana. There, crime rates have increased, and social services are diminishing. She is a part-time retail worker with unpredictable shifts, unreliable transportation, increasingly expensive childcare, with a previous history of substance abuse. She is also far from close family members.

In her life, Lisa has experienced a series of personal relationship setbacks. With few options for reliable, well-paying employment, Lisa is dependent upon government benefits for her and her child's survival in low-income housing.

Lisa's example shows the following vulnerabilities

- A "perfect storm" of erroneous information in government databases and unreliable internet access due to local power grid outages. Disputes with digital payday lenders has also resulted in Lisa not being able to access the meager funds she needs to pay for expenses.

- The creditor for her car has remotely deactivated it, and she is forced to walk as even public transportation requires digital payments.
- Government service algorithms have determined that her financial life patterns are endangering her child and instruct the dispatching of Child Protective Services to place her son in temporary foster care.

In summary, the convergence of digital payments that dominate her life, and the over-reliance on AI to allocate services and civil punishments, has left her destitute and hard-pressed to improve her situation. She has become one of the "digitally disadvantaged". Any attempt by relatives to provide funds are fleeting because as soon as the funds hit her digital wallet, they are seized.³⁰

In this threat example of digitally-issued benefits and loans, it's evident that there are extreme vulnerabilities in a completely cyber-enabled social safety net of products and services. Lisa is part of a VC with little support and a fragile day-to-day existence. Her socioeconomic condition and over reliance on a digital infrastructure make any disruption (e.g., criminal, environmental, conditional, etc.) highly dangerous. The very nature of the cyber-enabled social safety net makes the VC more vulnerable, and the cyber portion acts as an amplifier of the threats, the risk, and the impact.



INDICATORS (FLAGS)

FLAGS DEFINITION

The Threatcasting process maps out possible and potential threats 10 years into the future. It also identifies the “flags” that indicate a specific threat future is underway and/or may come to pass. Sometimes referred to as “signals”,³¹ they can give an early warning that a potential attack is in-flight or beginning to form.

GENERAL CEFC TRENDS

Flags can be categorized in multiple domains (e.g., technical, cultural, social, economic, regulatory, etc.). Each flag described below is a micro-indicator that the threats outlined in this report are emerging. They are often built off of one another, and by doing so, provide multiple early-stage indicators to prepare for the threat

1. Improved Detection and Attribution:

This flag is a natural evolution of current AI transparency, research, and policy as well as a gatekeeper action identified in the next section. The threat futures from the workshop indicate a need for detection in small-target financial crimes, especially those enabled by AI. When scaled to the masses, AI-enabled crime becomes a tool for nation-states and their proxies. For instance, the more that AI is involved with crypto transactions, the faster their speed, scope, and scale. This can rapidly escalate, causing market fluctuations that appear to be at the level of economic warfare - even if the intent was not to cause economic warfare effects. Because of the ubiquitous use of algorithms in financial systems, there will naturally be a buildup of technologies to improve detection and attribution of financial transactions and illicit behavior.

2. Lagging Technical Knowledge:

For the foreseeable future, the technical knowledge of the average public about crypto and digital economies is expected to

remain low. The speed at which new digital coins can be minted sets up opportunities for unaware users to be lured into a scam, fraud, and/or losing proposition. This will be even more apparent as developers attempt to innovate the next type of virtual currency or decentralized finance (DeFi) platform to attract new investors.

3. **Speed, Scope, and Scale:**

The development, adoption, and innovative uses of cryptocurrencies, decentralized ledgers, blockchain contracts, and other elements of DeFi technologies will explode in scope and scale. The speed of these algorithms may require new mathematical and cryptographic models.

4. **Attraction of “Un-Reality:”**

It is anticipated that there will be growth in the attraction to what the Threatcasting Lab calls “un-reality” or the belief that a technology, such as digital currencies, crypto investment, virtual reality worlds or online communities will automatically solve societal concerns, such as economic instability and discomfort in social situations. Un-reality attempts to replace real life with a constructed vision of a comfortable life that ignores the imperfections and failings of being human and living a human existence. Those seeking a new reality through technology might promote the growth of policies and laws that overlook basic human rights. Those seeking to escape the realities of

life might also spend unhealthy amounts of time, money, and attention on virtual existences that ignore international politics or ethnic and nationalistic conflict. Aggressor nation-states looking for opportunities to exploit another country's vulnerabilities may seek to change realities to match their desired world views. Often this has been and will be achieved through misinformation campaigns that influence the target(s)' understanding of reality for strategic advantage.

5. **Thwarting Identity Verification:**

One of the most troubling flags will be an attempt to alter, subvert, gain control over, or bypass identity-verification methods. Considerable resources are projected to be allocated toward efforts to influence people to part with their private keys or seed phrases. Similarly, there are currently bots watching the crypto exchanges for specific fluctuations, offerings, and contract executions - sometimes called front runners - that are programmed to seek out opportunities before the rest of the network has the ability to catch up.³² While a front runner bot may not technically bypass identity authentication measures, it may be able to move faster than the consensus protocol and create transactions that are unfavorable to one party – simply because the party trusted the verification methods of the network to be completely safe.

31 Webb, *The signals are talking: Why today's fringe is tomorrow's mainstream*.

32 Samczsun. *Escaping the Dark Forest*.

6. All or Nothing Technologies:

Another flag with deeply concerning implications occurs with all-or-nothing shifts to certain technologies that lack a way to revert to an earlier known preferred baseline state. Digital banking, online shopping, and personal smartphones are examples that demonstrate adoption of technologies that are largely irreversible. This will increase the divide between those who can adopt technologies knowing the implications, and those who are forced to make the change and are disadvantaged because of it. This will also likely increase the number and scope of venture capitalists.

Additional trends that might influence the CEFC environment include:

- Increased breaches of health data, such as biometrics that is useful to bypass authentication controls.
- Non-universal adoption of updated industry standards and practices.
- Centralized processing of digital currencies as opposed to decentralized intentions of cryptocurrencies.
- Social conditions breeding new scammer variants.
- Expanded reliance on Chinese services, technologies, standards, and policies.
- Unexplainable crypto-asset value fluctuations.
- Hidden real intent within information campaigns.
- Sponsored digital currency "hackathons".

- Formation of new online communities (e.g., pro- and anti-digital currency, centralized vs. decentralized control, NFT marketplaces).

CONDITIONS

Workshop participants joined with post analysis staff to gather and document a wealth of conditions and specific indicators that will enable CEFC. These conditions differ from flags in that they are much broader, generally overlap, and can be subjective. These conditions provide a broader range of areas to monitor the progression of the CEFC environment and possible threats.

CEFC Conditions

- **The Emergence of Well-Funded Adversaries** - An increase in funding for bad actor(s) - whether from larger criminal collectives, due to the lucrative nature of the CEFC environment, or from nation-states who want to engage in economic warfare.
- **Reliance on Digital Only Payments** - A shift from a hybrid, digital, and physical approach to digital only payment practices in both government and industry.
- **Increasingly Robust Digital Personal Profiles and Information** - Along with digital payments, personal information is kept mainly in digital forms that can be traded, hacked, and purchased.
- **Adversaries Cultivating a Talented Workforce** - In the race for talented labor, criminals, and nation-states

increasingly recruit talent for the CEFC environment.

- **Lack of Understanding or Awareness of Digital Risks and Digital Security** - Driven by profit and convenience, industries and consumers continue to lack understanding of the threat space.
- **Interconnectivity of Applications with Disparate Information** - Expanding business and government use of the CEFC-vulnerable environment (e.g., IoT, 5G) also requires a connection with an increasing number of devices that gather information. Varied business practices and fragmented governance mechanisms cannot completely manage the risk of interconnected devices and massive data.
- **The Shift to All Digital** - - The CEFC environment becomes the primary space for daily activity, such as online banking, gaming, dating, and entertainment. Driven by industry, these spaces are monetized, and provide an easy entry point for consumers to engage.
- **Delays and Blindness to Hacks and Breaches** - The increasing complexity of the CEFC environment will provide cover for criminals and nation-states. As adversaries hide in the complexity of the environment, awareness of an attack could be delayed or obscured completely.
- **Increasing Ability and Tools to 'Spoof' Virtual Identity** - The collection of biometrics and use of AI, and other CEFC-enabling technologies, provides criminals and nation-states with a standardized approach to identity. This standardization will come from the industry and governmental needs to standardize use and costs. This

standardization will expand tools and services to spoof and hijack identities.

- **Lack of Safety Net Leading to Disparate and Uninformed VC Risks in Crypto Applications** - The increasing use of the CEFC-enabling environment gives VCs a fear of missing out, pushing them to "get in now or risk missing out" (e.g., investing in cryptocurrency and adopting new digital tech).
- **Persistence of 'Zero-Day Bugs'** - New bugs impact any system or application, which gives rise to a larger market to find them, exploit them, and/or sell the solutions.





ACTIONS TO BE TAKEN (GATES)



GATES DEFINITION

In addition to uncovering threats and flags, the Threatcasting workshop participants identified actions that could be taken to help mitigate, disrupt, and/or recover from the threats. These actions constitute a “whole of society” approach to problem-solving and have been applied to specific domain areas where detailed steps can be taken. To be most effective, the actions must be fluid to adapt and shape the future applications of technology.

GENERAL ACTIONS TO BE TAKEN

Organizations can take actions at two points in time: 1) before a threat event occurs to avoid, disrupt, or mitigate its effects, and 2) after an event occurs to increase speed of recovery.

Pre-event (Prevention) Actions:

Enhanced encryption for digital currency rollout - Four threat models from the workshop indicated a measured approach to how a nation should introduce a central bank digital currency (CBDC). This approach is proposed to emphasize encryption standards as part of the preventative defensive mechanism against criminal activity – presupposing that if the lock is strong enough, criminals cannot get in. This encryption-based approach implies locking up several things, such as personal data, the private key, and the currency itself.

Proactive regulation - A significant emphasis was placed on developing federal level regulation. Some of the specific regulatory recommendations included:

- Deliberate and clear reporting as well as an award process for individuals and companies that report financial crimes. This should include clauses that minimize retribution and retaliation against whistleblowers.
- A red line policy for conflict escalation against nation-state actors. Lawmakers must consider when the U.S. would be allowed to conduct military action against economic warfare efforts from a nation-state or its proxy.
- A robust insurance industry to compensate victims. There is a need for more studies about how the private insurance industry can be regulated to protect consumers from CEFC.

- Expanded sandbox opportunities that are modeled after financial technology (FinTech) experiments to understand the implications of CBDC, crypto investment, and other cryptocurrency applications.
- Agile government regulation practices, specifically designed to increase resiliency of cryptocurrency investment and smart contract markets.
- Leveraging non-governmental sources to assist with regulation. Several of the threat models included increased U.S. participation with world banking systems as a necessary step to stabilize the multinational ripple effects of digital financial crimes.

Identity management - Identity management technology and policies were at the center of several threat models. This topic relates to current “know your customer” (KYC) requirements for the cryptocurrency economy, although future financial crimes will attempt to circumvent KYC policies. What may improve the visibility on the lack of KYC standards for some CEFC applications include an improvement to background checks and the designation of identity verification as a “National Critical Infrastructure” to accompany power, transportation, and water. By doing this, the seriousness of long-term threats to national security taking place through cyber-enabled financial crimes is addressed.



Detection technology and policies

- This is arguably the largest category of possible actions recommended by the workshop's threat models. Much of the detection of CEFC must be done automatically and algorithmically. Most models used broad wording to describe detection, which in laymen's terms, essentially means "figuring out a way to see the bad guys doing bad things". Other recommendations include:

- The development of a "financial crimes analysis science". This might be a branch or extension of threat finance science, or how analysts and detectives "follow the money". Purposeful training and university degrees could combine network science, AI-assisted triage, and intelligence procedures to make detection and recovery much faster.
- Before smart contracts are executed, apply algorithmic detection by developing tools that monitor contract attacks and learn how to triage the threat, contact key decision makers, and isolate the malicious ones. For example, the article, "Escaping the Dark Forest" provides details of how a volunteer vulnerability researcher mobilized his contacts to recover nearly \$10 million dollars in threatened cryptocurrency in less than 24 hours. This is the speed and type of response that federal law enforcement must aspire to in order to stay ahead of future criminals.

Education - Almost half of the threat models from the workshop recommended some type of user-level education program. Mostly, the models imagined how criminals might take advantage of gullible and vulnerable people. This likely correlates to the high amount of theft and fraud crimes that are directed at individuals at the small financial crime end of the ladder. As a preventative measure, much more education is needed on unique cryptocurrency, digital economies, and the threats that come with these technologies. Actions will need to go beyond "digital literacy" and "digital hygiene". The recommendation included additional research to discover better ways to protect individuals from CEFC.

Understand the emerging environment - As digitalization continues to move real-world value to digital assets, it's necessary to understand how to describe the changing environment, including how to apply legal concepts to digital spaces.

Maxim Kon, CEO of Cheksy, a blockchain investigation and compliance consulting firm in Switzerland, currently sees non-fungible tokens (NFTs) as a high-risk category of digital assets that eases money laundering operations. He recommends a number of actions be taken to reduce the impact of money laundering through NFTs including:

- Regulators and forensics analysts carefully watching NFTs as a separate

type of crypto asset.

- NFT marketplaces implementing an industry standard KYC and Anti-Money Laundering (AML) policies.
- NFTs being regulated, so that they cannot be generated anonymously.
- Metaverse and the online gaming industry thinking ahead about the impact of NFTs and how these industries may play a part in the future of AML.³⁴

During/Post-event (Consequence Mitigation/Recovery) Actions:

"In-the-moment" actions – Actions recommended as the threat event occurs:

- Provide a counter-narrative or an "official" perspective about what is happening, keeping in mind that this is also the same space that disinformation campaigns flourish. While trying to act in the window between event and post-event, the messaging should rely on the science and best practices of counter-disinformation. Creators and distributors of the information should also anticipate the consequences of counter-counter-narratives.
- Establish and use clear requirements and channels for reporting. Clear reporting must be accompanied by trust that action will be taken to remedy the current situation and create a

33 Samczsun. *Escaping the Dark Forest*.

34 Kon and Cheksy, *NFTs: The ultimate money laundering tool?*



sense that retribution against those victimized will not be tolerated. In other words, victims of ransomware should be confident that they can turn to a specific named agency and not be penalized for reporting a crime.

Return the "system" to pre-attack functionality

– The following actions are recommended to be taken to improve functionality:

- Employ data redundancy and data backups as technical tools to allow companies affected by a financial attack to restore some sense of functionality. It is not clear how this would work for individuals.
- Develop an “analog currency” backup available to restore functionality if a digital currency has technical difficulties. This implies having the ability for an individual to have “cash under the mattress” in the event of an emergency, but what this scenario looks like in a fully digital economy is unclear.

Enacting justice – This is the most varied category of recovery and may not have immediate ties to the original financial crime that perpetrated the loss. Recommendations include:

- Develop mechanisms for threat attribution and the rehabilitation of former criminals with a focus on the actor part of the triangle.
- Recover personal assets through

insurance payments, federal stimulus payments, or identity recovery procedures that represent the second part of the Crime Triangle. Using insurance as a recovery method implies (and demands) that the insurance industry be prepared to tackle crypto and the fallout from future financial crime. It also implies that the insurance industry has studied the ways this could happen and has assigned risk assessment scores. Any discussion of insurance as a recovery plan of action must also assume that steps need to be taken before the event to set up the processes and procedures. This could occur through traditional markets or deliberate federal programs.

- Develop plans and possible actions the government would take to retaliate against economic warfare. For instance, are there policy red lines that would authorize military (e.g., cyber and kinetic) actions or economic warfare actions against a nation-state or proxy? While not discussed in the workshop’s threat models, current policies in cyberspace warfare could be relied upon as a baseline.

ACTIONS SPECIFIC TO FEDERAL LAW ENFORCEMENT

To disrupt and mitigate these threats, Federal Law Enforcement should consider:

- Utilizing a functional definition of CEFC technology and adjacent practices. The definition should include an understanding of the distinction between traditional financial crime and new crimes - where the increased impact, speed, scope, and scale of CEFC will expand to impact Federal Law Enforcement.
- Empowering, protecting, and performing outreach to VCs (e.g., consumers, companies, computer systems) with lawful monitoring systems that understand the importance of identity, confidentiality, integrity, and availability.
- Tracking and monitoring emergent CEFC through the sharing of best practices across federal and local law enforcement, as well as the DoD. In addition, specifically:
 - Determining how to identify if the attack behind the financial crime masks a broader nation-state attack.
 - Developing processes to pass the identification and intelligence of the CEFC from law enforcement to DoD when jurisdictionally appropriate.
- Further exploring CEFC's "pre-crime conditional state" with indicators to watch for and actions to take. This type of approach has been used for other conditional states, such as natural disasters (e.g., hurricanes, wildfire, etc.) to identify vulnerable people and situations that might see an increase in specific crimes (e.g., identity theft, fraud, etc.).
- Treating crypto like property, as described by Aidan Larkin, CEO of Asset Reality. He shared insights that courts are treating crypto as property, which can be seized and recovered to generate income just like any other seized asset. With that said, officials who seize crypto assets must create a plan for storing and safeguarding this type of property. Larkin likened the seizure of crypto to recovering a stolen high-end piece of art, "...you don't just throw a Rembrandt or a Banksy into the back of a police van." Agencies must develop storage and transfer procedures that are secure and accessible at the point of seizure, so that the crypto is immediately locked down.³⁵

³⁵ Larkin, *Demystifying crypto asset recovery*.



FURTHER READING

1. **Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides** - news, expert commentary, and information on Bitcoin and the Bitcoin blockchain technology.
2. **Blockchain Data Platform** - a for-profit company that provides blockchain analysis services and regularly conducts independent research on key crypto, blockchain, and digital economy issues.
3. **Cryptocurrency and Fincrime Compliance** - getting started, going deeper, investigation tools, including searching the blockchain ledgers.
4. **DOJ Seizure AUG2020** – great vignette about DOJ and crypto / terror financing.
5. **Financial Action Task Force** – multinational watchdog trying to set international standards.
6. **Financial Crime Academy Blog** - Compliance, Anti-Financial Crime, AML - blogs of different types of financial crimes.
7. **Tech Against Terrorism** – a great platform that releases a lot of content about tech + terrorism. Often outside the blockchain space, but some overlap.
8. **Web3 is going just great** - blog and analysis of current events in crypto, NFT, blockchain world.





SUBJECT MATTER EXPERT INTERVIEW TRANSCRIPTS

This appendix contains the unedited (and machine transcribed) transcripts of interviews with five subject matter experts. The few edits we made were to correct fundamental mistakes that changed the meaning of a sentence. These experts provided their opinions on the trajectory of various trends in the cyber-enabled financial crimes environment. Their opinions are based on their own academic research, industry-related expertise, and leadership observations.

The interviews recordings were made available to workshop participants as inputs to the effects-based modeling phase.

Anne T. Griffin, Columbia University

So, I have, I have a couple thoughts. But one area I wanna talk about today is in the realm of like digital assets, which can be crypto, it can be NFTs. It can be like any digital assets, but I'll probably touch more on crypto today. And some of these things are problems we're starting to see now, but they are on a smaller scale because right now, like for example, like most, most of my money is in traditional us currency. Right? Not, not a big issue. Like, you know, it's in a bank, it there's some sort of, you know, it's, the bank is insured. Like that's, that's not an issue. Right. But we're start what we're starting to see. And hopefully some of the people who are watching this are somewhat aware of are these scams where people are getting like scammed either out of their cryptocurrency or people who have cryptocurrency are getting robbed.

So, like on the small scale, like I used to work at a blockchain startup. A lot of people have crypto or well, and criminals also assumed that people working there had crypto. So, they would do the scam where they take over your phone and they try to hold of like, you know, all your apps and that kind of thing, and your wallet to get access to your crypto. So, they can steal your crypto. And, you know, once you do a transaction with most crypto, that's

not a reversible action when we're talking about like decentralized cryptocurrencies, and we're starting to see again, this is usually like targeting certain individuals that is bad. But most of the time it's like, oh, maybe you got like a couple thousand dollars from this person. Most people who have a couple of thousand dollars in crypto right now, it hurts to lose it, but it's not the end of their world.

Right. Where I think we're seeing in what we've seen since, like, I think it's 2012 when the Bitcoin white paper came out is despite the fact that we keep seeing this as a fringe technology, we're only seeing the adoption pick up and we're starting to see, you know, the, the concept of digital central banks, which means that we're going in a direction, not saying that crypto is gonna replace all currency, but it's gonna become a lot more commonplace and like an option, like how Visa, MasterCard, like anyone who qualifies, you know, either for a debit card or credit card has one, if they can use it because there's so many places now that are cashless, right. And we're gonna get to a place where, you know, you don't have to pay in crypto, but it is an option. And like possibly a very prevalent one.

And what I really see this as is when we get to that point, whether that's five years from now, 10 years from now, is that theft on a much larger scale. And we're not really seeing, like I said, like one of the common ways is people will hack into someone's phone. We're not really seeing the cell phone numbers do a lot for security. There there's the pin, but I've also heard many stories of the cell phone company saying like, oh, well, whoever called us said they forgot their pin. So, it's actually like a fairly easy hack. And that's not really, there's not really a lot there that you know, the cell phone companies get in trouble for. And also it's, if we're talking about again, decentralized money that's not insured once it's gone. It is gone. For example, if someone got a hold of like both my checking and my 401k, they drained it tomorrow.

And there was like no way to reverse it. And it wasn't insured. I'd be in a lot of trouble. And, you know, while we're not necessarily seeing a ton of people putting their retirement assets as like digital assets as we're starting to see people's, I guess, like spending money or what they, what they pay bills or going out that kind of thing as becoming more of that as being handled with crypto, we're gonna be able to see a lot more people having, being targeted for crypto. Like the way we see a lot of people actually get their like credit card or debit card skimmed at a store. Well, it's gonna be so much easier if you wanna do something like that with crypto, because it's like, if I figure out like, you know, okay, this is that person's wallet. I can just take your, your crypto and you can't get it back.

So, we're gonna see that at a larger scale. And the other thing that I really see as a risk here is again, like, as there's increased adoption, we're starting to see like the larger institutions, you know, exploring like, okay, what do we do with digital currency? Some of

them are saying, we, we have our own digital currency, which would be centralized, which, you know, then that would probably, obviously they they're working a lot with, you know, legislatures and other people to figure out like, how do we do this in a way that's legal and safe. You know, and isn't like screwing over our customers, but they're also institutions who are figuring out how do we let our customers, like, let us like hold their Bitcoin. Right? And once we get to that state, it also kind of becomes a problem because again, traditional money goes bank to bank.

The banks are the intermediaries, but if the bank is like kind of an optional intermediary and it's like, well, I know let's say I don't, I don't understand how traditional crypto wallets work. I have JP Morgan Chase. I wanna get into this thing called Bitcoin. And I buy it through them and they hold it. Right. And then let's say somebody does something and they hack in and they're able to steal like the Bitcoin outta my account. Well, okay. If it's, if they are able to like hack into the, and specifically target the digital assets, right. That's probably gonna go to a private wallet. And once it goes to private wallet yeah. Like JP Morgan chase can probably find the identity of the wallet. They can send that to the authorities, but it's gonna be a lot easier for them to take it outta that wallet into a bunch of other wallets, which becomes like a big game with tag, which is a lot more work for them to follow that through a bunch of established banks that have, you know, known laws in different countries or wherever these bank accounts may be and like how they're going to handle this type of situation.

And also just rules about like how banks, I think there's gonna be the big question of like how banks will be insured, if at all, for like these type of digital assets. Because right now they're really handling things that are, you know, like fiat currency. And once we start thinking about things as like, you know, these digital assets where some of the use again are decentralized, but they are enough traction that people are gonna keep wanting to use them, even with alternatives of more centralized ones, like you know, central banks having their own digital currency. Those are things that we need to consider. And then I also think the other thing that we also are gonna see is when we have you know, Tesla very famous was like, we're gonna start accepting crypto. And I thought that was very interesting because I don't think they ever intended to accept crypto long term.

I really think that this was a short term thing because I think they wanted it as an asset, but they didn't wanna purchase any of it. And that's why I think they actually cut it off where they were like, okay, cool. Like we got what we wanted and we're, we're done now. We didn't have to purchase any of the crypto. It was just given to us. But the thing with that is depending on how Tesla did that, right? Like, I'm sure that's sitting in a wallet or wallets for Tesla, but does that now make them like, like a honey pot or like, does that make them a target because now you have this like a company that now has a larger amount of crypto

and there's again, like, I'm sure that they're doing a lot for security, but there are a lot of things where, you know, it, it is lot newer than how we've been dealing with, you know, digitizing banks with fiat currency.

And so I think will also be really interesting as institutions start accepting crypto them figuring out like, how do we, how do we best secure this? Because obviously if tomorrow you know, somebody took a big chunk of money from apple. Like, you know, Apple's probably gonna be fine, but that's still not great. And that starts getting into, like, if you target it enough of these companies you know, that starts becoming somewhat of a national security of threat. If you're able to kind of say like, "Hey, we're gonna target like Apple, Microsoft, Google, whatever, for like, you know, their specifically their digital assets," like all at once and like do things that are gonna seize that up. So, there's a lot of things that I think you know, like cuz how it impacts the economy and some of our bigger like companies that it becomes like really complicated.

And I also think that the laws will also need to catch up in terms of like, how, how are we gonna handle this? Because the adoption is continuing to climb. I don't see countries like the us, like banning this or outlawing this. And frankly at this point I think would be a big mistake if they did that. But like, you know, the laws and it's tricky because New York came along where it was like, "Hey, we don't want people doing this and we're gonna find you if you don't have a license." And people say that that really hindered innovation in blockchain and crypto in the state of New York when they did it. And it was kind of, they it's kind of agreed upon now that was too much regulation too early, but also too little regulation too late in this of once it becomes more mainstream, I think also has a lot of risks.

And there are other things where I also have seen where, you know, as you see more adoption, I really see the scam businesses that are saying like, "Hey, we wanna help you do this. We wanna help you do that" growing. It could get to that point in 10 years with crypto because you know, a lot of the people it's been around enough where it's like people who are about to be middle aged you know, are starting to get into it. So, in 10 years from now, we're gonna have people where it's like, they're a lot closer to retirement than they are towards the beginning of their career. And they're gonna be like, oh man, I really need to like put some gas in, in my retirement. Right. You know, having gone through like two recessions in a pandemic and everything else, and you're gonna see like I'm gonna reference a local channel here, like on New York one instead of the, like get into this annuity thing, if you're getting retired or da, da, da, da maybe that's not a scam, but it's kind of like, this is towards people who don't really understand about investing on and like being on a fixed income.

And I really see that as like for people in some of the, in like millennial generation and some of the older gen Zs who maybe didn't quite catch on in this wave. And maybe didn't quite understand them being targeted towards like, "Hey, you're about to retire." There's a whole TV commercial. But by the time people realize it's like a scam, you know, the TV, commercial stop running, those people disappear. And if the laws and other things about these things don't catch up, you're gonna have people who are gonna be like, well, I was told if I put my retirement savings in an, in this thing that I would do great. I really see the algorithms, their biggest risk is we already see so many people excluded from our current financial system. And as things have been becoming more digital, like in terms of money, we are seeing that divide increase.

Because people are like, they don't really need to go to the ATM. So, you don't need an ATM on every corner. Right? Like sometimes I go places and they're like, oh, the nearest ATM is like way over there. Right. it's just not necessary to carry around cash with you anymore. And so, as things become more and more digital you know, there's also the decision making element where as we're introducing more algorithms into our financial systems, things where, okay, we're trying to now get these people who have been traditionally excluded and having the algorithms saying like, oh wait, no, like not that person, like they, they, they don't qualify for this or they don't do that. Or like they're too high of a risk. And I know there's companies out there that are starting things to try to mitigate that. But it's really like, the question will be like, how scalable is that?

Because there are so many people, especially people with our, you know, our whole immigration problem where they're paid only in cash and they really have no way to turn this pay fiat money into digital money and have that accepted anywhere. And also it becomes a problem of like them getting robbed and it's there become less and less avenues for them to be able to pay with cash, you know, they will continue to become excluded. And, you know, that puts that population at like you unique risks as we're using more and more of these algorithms, whether it's in, you know, individuals accounts or whether it's, you know, at a much larger trading volume for much wealthier people, I really see also the potential for, you know, that market manipulation and people not real it until it's like, oh, by the way, like six months ago, somebody messed with our algorithm.

And as long as your assets are fine, we're fine and you're fine. But also like that was probably not like a good thing. Because we're seeing, I think like the more famous one is the, like the more manual version of fit with like those Reddit threads and Game Stop [and] AMC. But imagine if, you know, you could do that on a much wider scale and manipulate markets, like in your favor, especially if you're like a nation state or like that kind of thing, or basically do something to crash, you know crash something, or maybe not, could maybe do a whole economy, but you could do a lot of bad things. At very inopportune times.

Dr. Lydia Kostopoulos, Technology Innovator

The question at hand is what will future cyber enabled financial crime perpetuated by either cyber criminals or nation states look like 10 years from now. But before answering that question, I think that it's important to reflect on where we are today in the financial world. Today, we have constant cyber attacks against banks against multifactor authentication on banking apps. And this is just the beginning of it. The core infrastructure of the financial industry is also being threatened [like] by attacks on SWIFT. This has really great implications, the international financial infrastructure, as we look to see what kind of future cyber crime we would have in the financial sector 10 years from now, we need to also understand where we are in terms of our industrial revolution. Right now, we're in the fourth industrial revolution. One that is characterized by IOT (internet of things), fast internet, 5g, AI, quantum, all of these technologies are changing the paradigm in which we operate across every single industry.

And because of that, we also need to rethink not just the way we do transportation, the way that we do medicine, but also the way that we do finance, the way that we exchange goods 10 years from now, we can imagine that we will see different forms of currencies, so cryptocurrencies, stable coins, but also state backed digital currencies. These will be very important in having a backup to the fiat currencies of today and that infrastructure right now that we do use today, that is threatened. So, what will the future of cyber enabled financial crime look like 10 years from now? The ideas I have are as follows: one, cryptocurrencies and stable coins, as these become more popular and used in conjunction with Visa credit and fiat currencies. This will be a type of finance that will be lucrative to steal by different cybercriminal organizations. Similarly, there are rogue nations who will seek to use cryptocurrency even more so that they can bypass the international system. This already exists today. But they will be able, they will be using this more and, and more in 10 years from now.

Two, looking at the fiat currencies, we talked about earlier, how right now the financial infrastructure we have today can be threatened quite severely by cyber attacks. And there is a need to go digital. There are nation states right now that are already looking into a digital coin or a digital currency that would be state backed. So, a national currency right now China's already experimenting with that as are other countries, 10 years from now, this will be a source of competition between nation states, but also an area where one nation could commit financial war against another nation by attempting to digitally attack or undermine the cyber currency of a different nation that is backed by a different nation.

Three, the ways that we are going to be authenticating ourselves to pay are going to be very different 10 years from now. We're going to be using biometrics our face, our eyes,

our fingerprints, but also we'll be using our mobile phones with different social media profiles that we can use to pay or other authentication methods that are internationally accepted, such as, for example, Apple Pay or Google Pay. And if, and when these organizations decide to create their own digital currency or own form of credit, this will really change the paradigm in which monetary goods are exchanged, but from a cyber crime perspective, stealing profiles will be very lucrative in this sense. Identity fraud will become much more serious when we start to use our bodies and our social media profiles or any kind of digital profile to pay for goods and services. The future is definitely hard to predict, especially in this current environment, but I hope these thoughts could be of use as you explore the potential threats in the financial cyber crime space. Thank you.

Mei Ling Fung, Chair of the People Centered Internet

We should be really worried about very enthusiastic people thinking here's better ways to make the world better. Because I was one of those people 30 years ago I had been at Intel and I was the alpha test user for that marketing system. And I had before been an assembler programmer. So, when Tom Sibel at Oracle came and said, we're going to reinvent business customer relationships. I said, I've already done it at Intel. And then for two years, I had the time of my life. <Laugh> really, as the pioneer of CRM, we did it, Tom Sibel sold it. It has now become a \$40 billion industry, but by the mid-nineties, the flaws were already starting to happen. But people were using this technology, which I had hoped would really benefit businesses and customers to exploit customer is to manipulate business management and, and some of these awful things.

The first one was customer surveys, which only asked questions where you could give high scores because the MBOs of the person designing it needed high scores. So, you never ask a question with a low score answer. That was just the beginning of what was just an awful nightmare. As I watched something, which I felt was my baby turned into a serial killer and that's what's happening now. And that's why I founded the People Centered Internet, cuz I needed to make sure that as we do the internet, we don't get too enthusiastic about the good stuff and forget about all the ways in which it can be used for bad purposes. There are extraordinary flaws in the internet as we have it. And whenever there's a flaw, it's just like a bridge. If you wanna bring down the bridge, you look for where themes are, where things might have gone wrong.

And all you have to do is wiggle a little bit there. And the whole thing will collapse. We are at that point of danger with the internet now because the internet was magic. It gave us an idea about what was possible when the globe was connected, but it was never designed to be fail safe, never designed to keep children safe, never designed for

old people, not to be exploited by scammers. All of this is happening. Now we have an internet that's built of straw. We need an internet that's built of bricks and that effort is not understood around the world. Right now, there is an effort by the UN to do digital building blocks that are the house of bricks. But you know, people are just going along thinking, oh, it works for me now. Just because it works now, nobody anticipated the impact that COVID would have on economies, on people's lives that potentially could happen with the internet.

I'm gonna give a FISO example at the very beginning of writing the invented writing, but the pushback was so great because it changed the powers, the authorities and who had the ability to invent the future that writing disappeared for 800 years before it could be reinvented. My real fear is that our communications are so fragile, even though they look so robust that we are not doing the hard work of making sure that they are what we need them to be for people to flourish. For example, you know, startups, isn't it wonderful startups. They make lots of money. You know, one of the most promising startups today, ransomware startups, yes, there's a ransomware village in Romania where if you wanna do a really good ransomware startup, you move to that village. It's written about in a book called Kingdom of Lies. And they have like shared call centers to explain to people how you change your, your money into Bitcoin.

So, you can pay the ransom. There's all, okay, what works, this works, that works. The other works. How do you get them to pay more money? It's a whole set up village to do that. We do not have the sheriffs in town to make sure that these kinds of things are spotted and eliminated. We are in that wild west magnificent seven time on the wild frontier, but gangsters are taking over whole communities because they don't have a sheriff and the lack of ability to come globally together on something like how, what do you do when you've got a ransomware attack that comes from an unknown country, we cannot organize ourselves. Why isn't cyber Interpol doing something about it? Well, it turned out that the head of CYBERPOL didn't know anything about technology. I know about this because the inside scoop in Singapore is that CYBERPOL has lots of money to hire great cybersecurity specialists. They all come to Singapore and then get hired by the banks because there's nothing to do inside CYBERPOL.

There's a total failure by institutions around the world to fix these problems. One of the reasons we can't chase down the bad guys is because the way the internet system of addressing is organized. So, it was organized for when there were 40 computers on the internet and all he needed was the CIS admin and the tech person and the admin person. And that's it. They never thought there'd be millions of computers on the internet. And that in fact, law enforcement would have to follow them down to try and find these ransomware companies. So, the DNS, [the] name system DNS, who's system is under the

control of ICANN – ICANN has abdicated responsibility for helping to improve it so that the right people can get the right information. ICANN is our job; [it's] what's public and what nobody can see that doesn't help chase down the bad guys. So, the People Centered Internet is really working on these kinds of fundamental issues.

Edmund L. Luzine, Jr., Ausable Funds

I think the first thing to think about is whether or not, if you are a criminal or some kind of other nefarious terrorist slap, or, or VEO violent extremist organization, do you want to use some type of crypto currency as the way in which to profit from your activities? And furthermore, do you want to use them in a way in which to invest or hold the assets you obtain through your illicit or illegal activities? And, and I think there's a mixed view on this. Obviously it is much easier from a physical standpoint to have digital assets to have things out there in the e-space however, there seems to be a growing problem with being able to access them and being able to access them when you want to and maintaining them.

So, for example you know, I think back to the original something that might have been competitive with this from many decades ago and that being bear bonds, you know, if, if you held the bond, the physical note, that was it, that was the equivalent of cash. You didn't need a code to find the bear bonds. You didn't need a computer to go and get the bear bonds. You either had them in your briefcase or in a closet or in a safe box, or maybe distributed in multiple locations around the world. So, the case at crypto you've got something, or, you know, whether it's Bitcoin or Ethereum or Doge Coin or whatever, the latest type of crypto currency is out there. You have some concerns about accessing it, and there have been multiple stories about people losing their passwords to accounts which is kind of unique.

The other thing is which, which you just saw from the hacking of the Colonial Pipeline and the ransom for it, which I believe was paid in Bitcoin, that the FBI was able to trace that Bitcoin and get some of the ransom back. I'm not sure if they're actually able to get all of it. So, if you are a criminal organization, would you really want to use extensively or rely on as your primary choice? Something like a Bitcoin. And I guess my thinking right now is no, you would not want to use that as, as your primary choice of, of an asset. And I, I won't, I don't think I'll call it an investment cuz you're not getting a return on it. It's not a security. Although it will fluctuate in value based on supply and demand in the marketplace for it.

So, you, you know, again, if I am a North Korean hacker group, if I'm a Bacan hacking group or Russian affiliated APT bear or whatever the term is for those groups, do I want all of

that Bitcoin traceable? And, and again, my thinking is, no, I, is that maybe one third, or once you get it, can you easily convert it to cash or to gold or, or something else and get it out of the electronic sphere where somebody can and track it or better yet where one of your colleagues in the group can steal it from you and then move it quickly to somewhere else. And then they just resign from your group or leave and move on. So, my thinking is that there are concerns, you know, going out over 10 years, how popular does this become?

Also which kind of cryptocurrency becomes more popular versus others. And those are kind of my initial thoughts on the use of crypto for hack, for cyber crime, for a nation state. So, I, I like when I look at all these digital assets, I like to have these discussions in the most tact and polite way I can. And, and I try to say to people, imagine if we could go back to World War II or in a, in another manner, imagine if you could bring the Nazi the party forward to now and your ability to identify people at ease based on a certain, you know, certain cultural, societal, ethno, religious group, and all these things like Facebook and LinkedIn and in China, WeChat, and all these other electronic platforms that people contribute to make it much easier for a nefarious government or an ill intended government, or quite honestly, parts within a government to ID people and target them.

So, if you are a nation state, you should theoretically be very happy with the movement of more assets in general, moving into the digital realm because number one, that makes it much more easier to identify people to segregate them. And also at the end of the day to either steal from them or, or quite honestly, as you see in the case with China right now, and the crackdown with technology firms, essentially to tax them more or in what China is saying to distribute the wealth or common prosperity. So, yeah, from the government side I think there are some very unique opportunities where they want to be able to digitally track or be able to tax people much easier with all of these different types of digital currencies or cryptocurrencies. Whatever. I mean, you could just go back and think and look at any kind of extremist type of government that's existed.

Let's say over the past a hundred years, whether it's a right wing fascist type of dictatorship, like in Chile or a left wing one in, in let's say Cuba or Nicaragua, if everybody's money were digital and you kind of controlled the pipes or the communication systems, you could be able to hack in and monitor all of that. Furthermore, you could also monitor all types of relationships between people and quite honestly, if you're the party in charge you could monitor also your opposition party or parties in their financial transactions and who is involved in each of those parties. So, I, I think it provides a very from that aspect, it, it provides a very unique opportunity to conduct surveillance or gather intelligence and see who find what and where, and almost in kind of the opposite argument.

You look at the challenges that the U.S. and allies have had over the past 20 years with terrorism, finance out of Afghanistan and Iraq and other parts of the Middle East and how those efforts have made more difficult through the hawala financing mechanism, which one could argue is almost the exact opposite of the digital, the various digital currencies that are now developing around the world. Hawala financing mechanism basically only allowed for currency exchange via a physical hard copy type of notebook or ledger that was maintained in different locations, not across the Middle East, but the world. So, unless you could get your hands on one of those, it wasn't like there was a there wasn't an electronic ledger in Google Docs that every hawala dealer could go online and update. So, it made it much easier for them to finance their operations and what they were doing.

I think there are a number of things to think about, and that is if you look at you compare something that happened in Panama trying to think how long ago the Panama paper situation was, but you had, and, and you also had a similar circumstance out of Switzerland, but you had the case where all of these electronic systems allowed for the concentration of records and files and assets and how disgruntled employee internally was able to take all of those records, duplicate them, and then hand them over to the press and let them know as to, in the case of Panama, how many government officials had accounts, how many had shell corporations and more specifically, which Panama still allows for how many had numbered accounts. So, and you also had that in Switzerland. It would be interesting to see if anything ever comes like this out of Dubai where you have the same type of disgruntled person in an Arab bank in the United Arab [Emirates] that would show how much money had come out of Afghanistan or out of Pakistan or out of other places had been thus far obtained.

So, there are, I think the one thing to leave with is that there are, there do seem to be a number of mechanisms developing and platforms that allow for it, for people to, or, or groups, financial criminal groups, or nation state groups to distribute their assets in much more different and unique places, whether it's through something like Bitcoin or somehow if they get a cash in some kind of application, whether it's through like a PayPal or a Venmo and they can easily move it around outside of the traditional banking infrastructure. I think that's a very unique thing to look at it as is something like a Robinhood trading platform that allows you to trade currencies and commodities and stocks very easily with low costs, if anything there's a whole bunch of things out there that are allowing people to do more like a better word, negative or nefarious activities at a very lower cost.

But again, I, I guess, so we get back to something, one common denominator besides the occurrence, the money aspect that all of these things had is that you need access to the internet and or to phone lines. So, that makes it very easy for a nation state to be able to

surveil and collect on. And it also would also, it would also make it easier for some type of group, not necessarily intercept those communications, but interrupt them through something as simple as, as just, you know, pulling the plug on systems that they couldn't operate or maybe jamming the actual transmission of data. So, the reliance only on the digital infrastructure, I think it makes it much easier to interrupt.

Ann Cairns, Mastercard

Well, first of all, let's start with the idea of the cashless environment. I mean, I think it's very interesting because we're still in the middle of the pandemic right now. And to a certain extent, what we've seen this year is a massive shift from paper based to electronic payments a shift that ever seen the size of in, in recent times. So, obviously that's really good news from some points of view and has driven consumers to behave in a completely different way. But also if you think about things like climate change coming onto, you know, becoming much more of a reality for us with the flooding and the fires and so on you could see a time where technologically having everything automated to the level that we do with no backup could be quite catastrophic economically and sociologically for society.

So, I do think that actually the recent shift that the pandemic caused you know, could be sort of bringing us into more of a danger area. If we actually aren't prepared to deal with all of the contingencies that we're gonna need to build in because of, you know, flooding and fire and, and, and so on. So, that's one thing that I've been thinking about recent. I had been in, in the investment bank and city during the first big crash in the eighties, '87 Black Monday in October. And in my time I spent the first year or two unwinding swaps portfolios and being involved in how you actually systematically reduce your risk across investment banking, but nothing of the scale of Lehman and what you saw in Lehman were lots of different things happening, different, a patchwork quilt of bankruptcy laws across the world, which actually didn't jive with each other.

So, different administrators making different decisions about how you would deal with different parts of the bank, which as somebody who was restructuring, the holding company was quite dramatic. The other thing that you saw was, you know, you would think that very good banks who were in control of their risk would immediately take action. And that is indeed what happened. We saw some of the sort of best prepared banks actually unwinding their positions with Lehman at a very, very rapid rate. But what actually transpired was that they were operating in the first, you know, few days and few weeks of the chapter 11 of the bankruptcy. And actually that was the most volatile period. So, while it looked like they were doing something that ha you know, was really good from

a mass risk management point of view financially, it was probably something which was a, a really could have resulted in much higher losses for them than if they had waited and unwind at a slower rate.

So, some of the things that you think intrinsically in the financial services industry –things you should do– are not necessarily, you know, the right answer in a sort of crisis situation. And at that time you know the, I don't recall what the level of algorithmic trading is, but I think there is a link here because if you are highly automated, and if you are into say algorithmic trading and something happens in the market then what you could have is a, is a whole raft of algorithmic decisions made in sort of split seconds, which would cause much rapid, more rapid financial instability than you could have experienced if you were actually in, in more of a manual trading environment. And I think that is actually a serious risk to find financial stability in the system going forward.

If and, and, you know, the, the thing about this is that if you think about it in respect of say cyber crime and so on if you start actually having big attacks on is that are linchpins in the system then you can bring down huge sways of the financial system without too much, too much further effort. If you see what I mean, what do I, what do I mean by that? Well, for example, when Lehman collapsed I, that something in the, in the swaps area, it was about 90% of the transactions were called what they call like over the counter. And only 10% of the transactions went through the clearing houses.

So, therefore there was a lot of bilateral risk system, but there wasn't the concentration of risk. However, when transactions actually go through a clearing house then, you know, there are all sorts of other protections that are built in there. A waterfall of risk management systems kick into play, obviously the different members of the clearinghouse put in a certain margin level. There are all sorts of different rules about how you operate there's skin in the game from the operators. And, and so on. So, allowing you to take action, if you saw one player, go down to be able to, you know, manage a default process without affecting the rest of the market. Having said that though, you know, you also have to have a view that says you've concentrated risk in a, you know, an area. And so now maybe you've got 70% of your transactions now being processed this way and 30% bilaterally, and that's gonna change your whole wholesale risk.

So, as individual players get hit, you know perhaps you're in a much safer environment to manage that. And I'm sure that everybody in risk departments across the financial space have learned a lot since 2008, 2009. But you know, if you hit a hope, if you hit something that's controlling everything, then you know, obviously that's much more serious. However, having said that the level of cyber securities, you know, investment in the hopes is, is massive. And similarly with MasterCard's network, you know to my knowledge and

MasterCard's network has never been breached. Although you hear, you know, things like, oh, Target --customers of Target-- had their information shared and so on, but that's not the level of actually hitting the network that is, you know, a, a specific user of the network. Similarly, banks have been breached. We know that by financial criminals and also by state actors.

But you know, you, haven't seen sort of a major hub breach in recent times as far as I'm aware. So,, so because I, and I guess that the reason for that is that it's the layering really it's, you know, it's the outrunning, the lion <laugh>, I guess that it's easier to breach the, you know, the players who are less protected thinking about the infrastructure of the future, you know, who is actually providing the, the componentry and the ability to operate the infrastructure of the future. And what could they do with that? If the, if you were more in a state of war kind of situation, that would be pretty scary, quite honestly. And I, I think that everybody's thinking about that right now. And in respect of not just things like 5G, but it's also things like nuclear power and so on, [not] necessarily weapons per se, but things that can be turned into weapons.

And I think in the space of the next 10 years, well, I think actually right now everybody's diversifying their supply chain, and it's not just because of, you know, sort of criminal threat or state actor threats, but it's probably a good thing to do because we've probably become a bit more complacent about supply chains than we needed to be, because we haven't designed them you know, to, to cope with things like COVID or even ships getting blocked in the canal, right? So, it comes down to you're living in a digital world, but actually the physical componentry of the things that you need to operate in a digital world you know, have to be thought about as well as the general sort of health of the, the population that, you know, are operating your systems and maybe even using your systems, because, you know, we say you can't be successful at MasterCard.

You can't, you can't be successful in a failing world. So, let's, you know, our products and services reach 3 billion people on the planet and our whole, you know, infrastructure operations. And the way we run our business is all predicated and designed on that. It was also, you know, designed to cope with an incredible amount of cross border travel and so on and so forth, which has gone away, but no doubt will come back at some point. And the point about this is that, you know, if whole sways of, you know, populations get affected by one thing or the other, you know, either by crime, either by, you know, pandemics either by global climate change, then big pieces of your business and big pieces of your supply chain could actually be impacted. So, I think that's, you know, that's certainly gonna be happening more and more and more as we go into the future.

The other thing about the future is yes, people are thinking about big global systems

and their, you know, governments and state actors are thinking that they want more localization certainly of their data. And I think that affects you as a global player. There could be pluses and minuses to that, of course, because, you know, if you are, if you are more if you're more flexible in terms of the way that you've designed your networks, and you've got very many nodes there and that one node could pick up from another node, then if, if nodes say in a country was attacked and you had an ability technically to shift to another node quite quickly, that would be a good thing to, to help you attack, you know, to help you prevent you know, fraud and, and crime. And so on. Artificial intelligence of course, is, is probably, you know, the most important tool that we've got in our arsenal right now to, to address fraud because we, we deal with up to a billion transactions a day in MasterCard, and there's no way that we could process those in real time and do fraud checks without artificial intelligence.

And the thing about artificial intelligence is I think that it's now used at a level, which is still sort of pretty mundane in my view. In other words, it's not really intelligent yet. And, but with the advent of 5g, the advent of quantum computing, it's going to change dramatically. And I think sort of the intelligence of being able to see something and analyze it and detect it and, and sort of stop it spreading will be there. But at the same time, the cyber criminals are really smart and they're, you know, they'll be using artificial intelligence to do exactly the opposite. So, it's, it's a chess game. I mean, it's always gonna be a chess game, isn't it? And you know, you're gonna have to put massive investment in to actually stay that one step ahead. That's presumably what we're trying to do all the time now. So, it's gonna be a very interesting world from that point of view.



Visit threatcasting.asu.edu for more information





FUTURE IMPLICATIONS OF EMERGING DISRUPTIVE TECHNOLOGIES ON WEAPONS OF MASS DESTRUCTION



A Threatcasting Lab Report



The views expressed in this technical report do not necessarily reflect those of
NATO or its member nations.

FUTURE IMPLICATIONS OF EMERGING DISRUPTIVE TECHNOLOGIES ON WEAPONS OF MASS DESTRUCTION



Analysts:

Brian David Johnson – ASU
LTC Natalie Vanatta – ACI/USMA
LTC Jason C. Brown – ACI/USMA
Greg Lindsay – Atlantic Council
James Carrott

Munaf S. Aamir, Sandia National Laboratories
Kiril Avramov, Director of the Global (Dis)Information Lab at The University of Texas at Austin
Samuel Brackett
Eric Bruijn
Dawn Brotherton, Army Cyber Institute
COL Cagri Caglayan, NATO
MAJ Aaron Cross, Department of Military & Strategic Studies, USAFA
Lt Col Peter Dahl
Nikhil Dave, Arizona State University
LTC Antoine d'Evry, NATO
LTC Hugues Didio, NATO
William DiRubbio, USAF
Adam Gabriele
Denis Garman, Chief Strategist, Lockheed Martin
Nancy Kay Hayden, Sandia National Laboratories
Mica Hall, PhD
Hadder Hussein, Texas A&M
Lexie Johnson, US Cyber Command
Elizabeth Kistin Keller, Sandia National Laboratories
Prof. Vilma Luoma-aho, School of Business and Economics, University of Jyväskylä, Finland
Josh Massad, Deloitte Futurist
Onege Maroadi
John Marx
Rory Moran, Mastercard
Lt Col Andrew Mitchell, NATO ACT
Eduardo D Monarez
Nathan Romeo, Norwich University
Alex Ruiz, Phaedrus LLC
Captain Allen Siegrist, USN
Todd Stratton, Phaedrus LLC
Mikaela Sullivan, Virginia Tech
Commander (DEU Navy) Dietmar Teufel, NATO HQ SACT Innovation Branch
N. Jed Todd, Deputy Lead Information Warfare Cross-Functional Team for Air Force Futures
Lynda Toumi
Jasmine Valentine
Lena M Young
Anonymous



Arizona State University Threatcasting lab

The Threatcasting Lab at Arizona State University serves as the premier resource for strategic insight, teaching materials, and exceptional subject matter expertise on Threatcasting, envisioning possible threats ten years in the future. The lab provides a wide range of organizations and institutions with actionable models to not only comprehend these possible futures but as a means to identify, track, disrupt, mitigate and recover from them as well. Its reports, programming, and materials will bridge gaps, and prompt information exchange and learning across the military, academia, industrial, and governmental communities.



TABLE OF CONTENTS

PARTICIPANTS	6
TABLE OF CONTENTS	8
EXECUTIVE SUMMARY	10
INTRODUCTION TO THE THREATCASTING METHODOLOGY	12
BACKGROUND AND DEFINITIONS: EDTS, WMDS, AND THE WORLD IN 2040	14
THE WORLD IN 2040	15
WEAPONS OF MASS DESTRUCTION	16
EMERGING DISRUPTIVE TECHNOLOGIES (EDTS)	19
WMD EFFECTS	21
DETERRENCE	22
INTEGRATED DETERRENCE	28
NORTH ATLANTIC TREATY	29
FINDINGS	32
FINDING #1: GEOPOLITICAL CONFLICT ESCALATION	33
FINDING #2: LOWERING THE BAR	34
FINDING #3: NEW INSIDER THREATS	35
FINDING #4: WMD EFFECTS	36
FINDING #5: DESTABILIZING CRITICAL INFRASTRUCTURE	37
FINDING #6: THE LONG GAME	38
BACKCASTING	40
FLAGS	40
MOTIVATIONS	60
ACTIONS TO BE TAKEN	64
IMPLICATIONS	82
OVERVIEW	82
IMPLICATION #1	83
IMPLICATION #2	86
IMPLICATION #3	88
IMPLICATION #4	91
IMPLICATION #5	93
IMPLICATION #6	96
IMPLICATION #7	98
A NEXT GENERATION OF INTEGRATED DETERRENCE	104
CONCLUSION	106
APPENDIX I – EDT EXPLANATIONS	108
APPENDIX II – SUBJECT MATTER EXPERT TRANSCRIPTS	120
APPENDIX III – A HISTORY OF THE NATION-STATE	148
APPENDIX IV – TOPICAL BIBLIOGRAPHIES	154





EXECUTIVE SUMMARY

RESEARCH QUESTIONS

What are the future implications of Emerging Disruptive Technologies (EDTs) on the future of Weapons of Mass Destruction (WMD) warfare? How might EDTs increase the lethality and effectiveness of WMDs in kinetic warfare? How can civic leaders and public servants prepare for and mitigate projected threats?

Problem

In the coming decade, state and non-state adversaries will use EDTs to attack systems and populations that may initiate and accelerate existing geopolitical conflict escalation. EDTs are expected to be used both in the initial attack or escalation as well as a part of the detection and decision-making process. Due to the speed of EDTs, expected confusion, and common lack of human oversight, attacks will also be incorrectly attributed, which has the capacity to escalate rapid geopolitical conflict to global military conflict, and ultimately, to the use of nuclear WMDs.

The use of EDTs in the shadow of nuclear WMDs is also expected to create an existential threat to possible adversaries, pushing them to “lower the bar” of acceptability for using nuclear WMDs. EDTs will enable and embolden insider threats, both willing and unknowing, to effect geopolitical conflict on a global scale.

In addition, the combination of multiple EDTs when used together for attacks will create WMD effects on populations and governments. Furthermore, EDTs will be used by adversaries to target and destabilize critical infrastructure systems, such as food, energy, and transportation, etc. that will have a broader effect on populations and governments. EDTs will enable adversaries to perpetrate a long-game attack, where the effect and attribution of the attack may not be detected for an extended period – if ever.

Solution

To combat these future threats, organizations will need to conduct research and intelligence gathering paired with exploratory research and development to better understand the state of EDTs and their potential impacts. With this information, organizations will need to conduct collaborative “wargaming” and planning to explore a range of possible and potential threats of EDTs. The knowledge gained from all of these activities will inform future training and best practices to prepare for and address these threats.

Organizations will also need to increase their investments in EDT related domains, necessitating countries to not only change how they fight, but also evolve their thinking about deterrence. Expanded regulation, policy making, and political solidarity among members will take on an increasingly more significant and expanded role. Broader government, military, and civilian cooperation will be needed to disrupt and mitigate some of these future threats in conjunction with broader public awareness. All of these actions will place a higher value on cooperation and shared resiliency among NATO members.



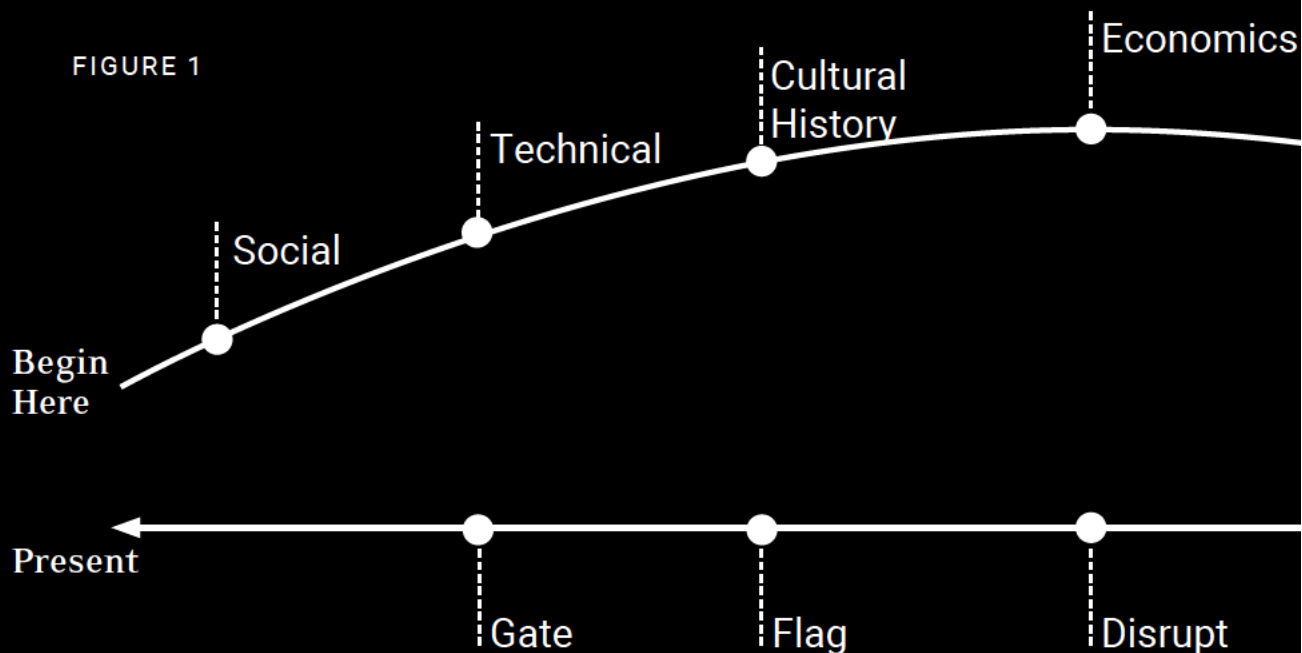
INTRODUCTION

INTRODUCTION TO THREATCASTING

Threatcasting is a methodology used to help multidisciplinary groups envision future scenarios. It is also a process that enables systematic planning against threats for up to ten years in the future. Utilizing the Threatcasting methodology¹, groups explore possible future threats and how to transform the future they desire into reality while mitigating a set of threats.

Threatcasting is a continuous, multiple-step process with comprehensive inputs. They range from social science, technical research, cultural history, economics, trends analysis, expert interviews, and science fiction storytelling. These inputs inform the exploration of potential visions of the future.

FIGURE 1

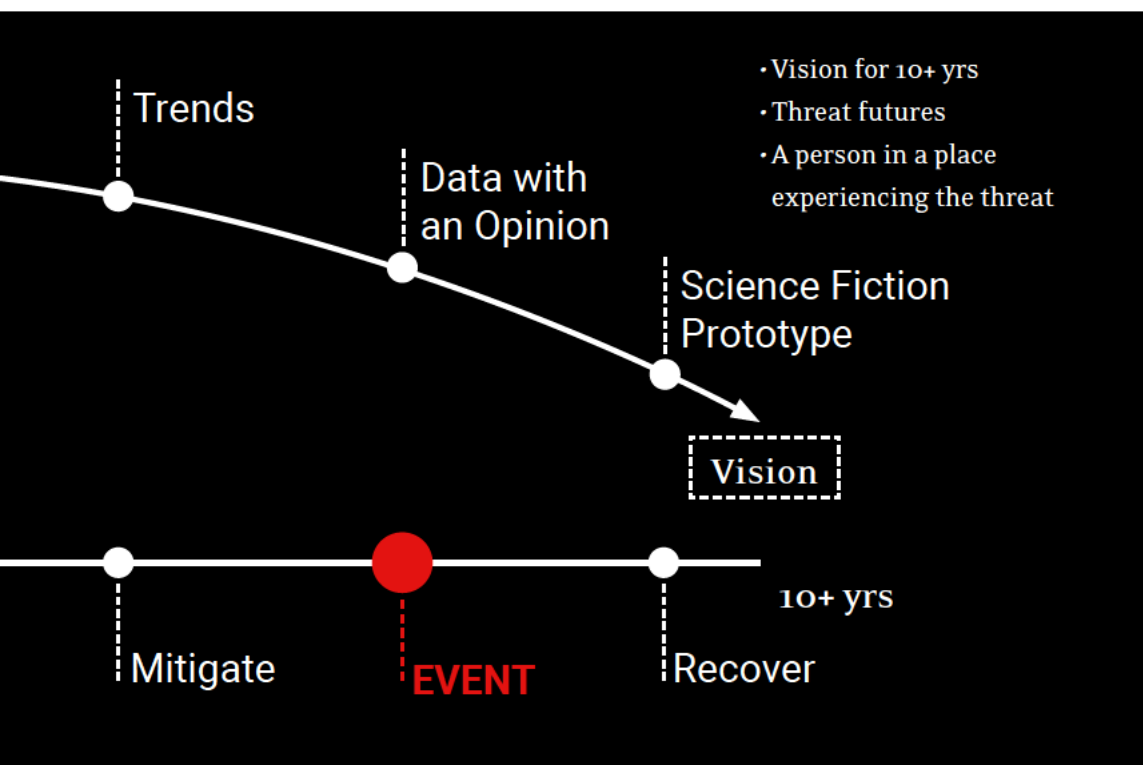


A cross-functional group of practitioners was gathered for two days in March 2022, to explore the future of WMDs and EDTs. The outcome is the beginning of a set of possible threats, external indicators, and recommended actions, that if taken, are expected to mitigate the threats. The projected outcomes, etc. are not definitive, but they give the organization a starting place. Participants synthesized the data into workbooks by drawing research inputs from a diverse data set of subject matter expert interviews and then conducted four rounds of Threatcasting sessions.

These Threatcasting sessions acted as simulations, which generated numerous separate scenarios, each with a person in a place, experiencing their own version of the threat. After the workshop concluded, analysts methodically analyzed these

scenarios to categorize and aggregate novel indicators of how the most plausible threats could materialize during the next decade and what the potential implications are for “gatekeepers” to mitigate the threats.

The output of the methodology provides organizations and decision-makers with a framework to plan, prepare, and make decisions in a complex and uncertain environment. Threatcasting often guards against strategic surprise. When a crisis occurs or an opportunity presents itself, a decision-maker or a leader is better prepared. With this, their response is more likely to be, “We have talked about this before. We know where to start...”





BACKGROUND AND DEFINITIONS

EDTS, WMDS, AND THE WORLD IN 2040

This report asks the question, “How might Emerging Disruptive Technologies (EDTs) increase the likelihood, lethality, and effectiveness of Weapons of Mass Destruction (WMDs) in kinetic warfare in 2040?” Before answering, it’s necessary to ask further questions, such as: What does the world look like in 2040? Who are the actors creating and escalating conflicts? What exactly are EDTs and WMDs?



In this section, we provide definitions, a background, and context to frame subsequent discussions of the findings, implications, and recommended actions.

THE WORLD IN 2040

While every strategic foresight exercise runs the risk of simply extending present trends, we can expect that the future will not be a case of “either/or”, but one more of “yes/and”. For instance, we can reasonably assume the world of 2040 will simultaneously be more connected and fragmented. While new information technologies continue to increase the speed, scope, autonomy, and interdependence of globally networked systems, the COVID-19 pandemic was a stark reminder of nation-states’ power to close borders, restrict travel, and use technology for biological surveillance and control.

Over the next decade, software and hardware will continue to relentlessly bombard us worldwide, becoming more deeply embedded in physical systems. In doing so, however, they will introduce systemic vulnerabilities and expand cyberwarfare attack surfaces to an unprecedented degree, producing an interconnected world that is also buggy, brittle, and hacked². In fact, it is entirely probable that cyberspace will be more fragmented in the future as authoritarian states increasingly impose sovereign digital controls and aim to separate from the global Internet.

The struggle for the commanding heights of technology will intensify, as nation-states and their private-sector surrogates race to stay ahead in such critical areas as artificial intelligence and quantum computing — where conceding advantage to a rival is apparent only after it’s too late. The rapid advances in these technologies — as recently seen in OpenAI’s GPT-3 and DALL-E 2 — will also empower individuals to an unprecedented degree, granting them access to tools that were unthinkable only a few short years ago.

This tension between connection and fragmentation will manifest in geopolitics as well. Great power rivalries will persist, as China’s rise and Russia’s invasion of Ukraine will alternately produce new spheres of influence, splintered technological systems, and isolated financial systems. These rivalries will be joined on the world stage by a new generation of super-empowered individuals, organizations, and other non-traditional actors, ranging from technology moguls to terrorist networks as well as groups knowingly or unknowingly manipulating people at scale through the use of selective misinformation.

This will, in turn, produce new adversaries whose motivations may defy traditional models of deterrence. Their activities and attacks will focus less on clear, legible military targets and more on civil and private infrastructure and institutions, such as healthcare, agriculture, and energy.

This is also expected to lead to the slow,

² Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*.

nearly imperceptible degradation of state capacity. In fact, many institutions will deny being attacked at all. In the past, civil critical infrastructure has been a target for adversaries, but the use of EDTs will allow for broader, multi-faceted attacks across multiple domains and targets to an extent not yet seen.

The same is expected to be true for climate change. By 2040, the mounting destruction due to climate disasters will be undeniable. Whether it will be extreme storms, heat, fires, flooding, and/or the impacts of rising temperatures, effects will be disproportionately felt by poor and marginalized communities (food scarcity and reduced access to health care). This will worsen social fragmentation, and further erode basic prosperity and security – also contributing to an overarching trend of pervasive volatility and instability in social norms and institutions whose resilience was once taken for granted. As new threats to both democratic societies and rules-based international order emerge, they will repeatedly test the adaptability of our interconnected global systems, ranging from the mitigation of carbon emissions to supply chains to public health. All of this will depend on a consensus reality that will be under attack.

Consider a potential scenario whereby another few decades of misinformation, individually-tailored media, AI-driven “deepfakes”, and the like will also wreak havoc on domestic and international politics. This may have the potential to

increase the strain on NATO nations in the absence of an explicit threat of kinetic warfare from a traditional adversary, such as Russia. By 2040, the military capabilities of NATO could be tautly stretched as the alliance faces concurrent requirements to monitor, police, and neutralize potential adversaries before they directly threaten Europe. This, in turn, could lead to NATO members being vulnerable to “strategic shocks” as military and civilian resilience is tested.

The world of 2040 is one in which EDTs threaten to exploit a connected world with a “strategic shock” that leaves it exceedingly fragmented.

WEAPONS OF MASS DESTRUCTION

Narrow definitions of WMDs include nuclear and radiological weapons (all types and yields), chemical weapons, and biological weapons. The United Nations refers to WMDs as a “class of weaponry with the potential to, in a single moment, kill millions of civilians, jeopardize the natural environment, and fundamentally alter the world and the lives of future generations through their catastrophic effects.”³ The United States Department of Defense defines WMDs as “chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties.”⁴

These definitions fail to capture the broader context of WMDs as weapons designed to both terrorize and deter. The very idea

of these weapons is “weaponizable.” This means the threat of deploying WMDs is often as effective as the weapons themselves (as it’s seen as a significant escalation of both political and military intent), which in turn causes a vastly greater hesitation to use them.

Images of poison gas, mushroom clouds, and horrific plagues deliberately and effectively enhance fear and confusion.

Nation-state and non-traditional actors alike typically resort to WMDs during long, painful, and involved struggles in which the mounting pressure to break a stalemate sufficiently erodes norms against their use and leads to further escalation.

The notion that WMDs are in a special category unto themselves is codified both in the elaborate models and doctrines designed specifically for their use (e.g., mutually assured destruction) and in decades of treaties against their testing, use, and proliferation. This also makes them ideal for false flag operations, conspiracy theories, and great power mind games used for strategic shaping. They are more often wielded as imaginary weapons to terrify and confuse, which only requires that rare examples be made. For example, even before dropping the first and only atomic bombs on Hiroshima & Nagasaki in August 1945, US Army Air Force (USAAF) created a WMD-like effect with the indiscriminate fire-bombing of Japanese

cities. Later, both the Cuban Missile Crisis and U.S. Strategic Defense Initiative (i.e., “Star Wars”) demonstrated how the threat to deploy or defang nuclear WMDs could alter the strategic and diplomatic global standing in an instant.

In addition to being an exceptionally powerful threat, WMDs are deadly weapons to the extreme. When they are combined with human manipulation, they become even more terrifying. As such, it may be the technologies of propaganda that most amplify their effectiveness and lethality. Not only does the threat of WMD use increase the likelihood of actual use, it also creates confusion about the definition of who and what are considered “legitimate” targets. This is where WMDs intersect with the increasing lethality and shock of such terrorist attacks as the 1983 suicide bombing of the U.S. Embassy in Beirut, the Tokyo Subway sarin nerve gas attack more than a decade later, and then in 2001 with 9/11. Strategic shocks such as these ultimately create a paradigm shift on how security and defense are considered.

Nature, of course, is the original WMD. Some of the largest mass casualty events have been natural disasters, such as the COVID-19 pandemic and the 2004 Indian Ocean. Today, the world faces climate change. At one extreme, there is the latest IPCC report that suggests a global temperature rise of 3.2C by 2050 and at the



other, nuclear winter. Recent efforts to model interactions between WMD use and climate systems suggest that even limited use — a mere 100 Hiroshima's worth of yield — would lead to catastrophic global cooling, with a subsequent shortfall in total food supply.⁵

WMD Weapons Platform

When this report refers to a traditional WMD, it is referring to the entire system required to design, manufacture, transport, store, command and control, target, and finally deliver that weapon to its target. In this context, the report explores how EDTs might increase the effectiveness and/or lethality of WMDs by addressing at least one component of such a system.

EMERGING DISRUPTIVE TECHNOLOGIES (EDTs)

As the title would indicate, Emerging Disruptive Technologies (EDTs) are an umbrella term for a number of disparate technologies that are both emerging — from the laboratory stage to a step away from mass production — and disruptive, in that they pose opportunities and challenges to the existing technological status quo. Taken together, EDTs possess outsized potential to

- 1) Accelerate conflict escalation and lower the bar for the use of WMDs;
- 2) Replicate and/or enhance the lethality and/or long-term destructiveness of WMDs when paired together or used in tandem; and
- 3) Offer dual-uses with defense and security applications.

What qualifies as an EDT? Definitions vary depending on which organization you ask.

NATO HQ, for instance, provides a number of examples of EDTs, which are considered the most disruptive. These include:

- **AI,**
- **Autonomy,**
- **Quantum Technologies,**
- **Bio-technologies and human enhancement,**
- **Hypersonics,**
- **Space, and**
- **Big Data.**

Additionally, two EDTs are potentially forthcoming:

- **Novel Materials and**
- **Manufacturing & Energy and Propulsion.**

Another list of “game changing technologies” by 2035 is offered by the U.S. Army Training and Doctrine Command (TRADOC), including the following list:

- **Robotics,**
- **AI,**
- **Computing (Quantum, Big Data, Sentient Data),**
- **Cyber,**
- **Additive Manufacturing,**
- **Electronic Warfare,**
- **the Internet of Things,**
- **Swarms/Semi-Autonomous Systems,**
- **Camouflage/Cover/Concealment/Deception, and**
- **Anti-Satellite technologies.**

Turn the clock ahead to 2050, and TRADOC adds:

- **Hypervelocity weapons,**
- **Synthetic biology,**
- **Power, and**
- **Directed energy weapons and energetics to their list**

A third opinion is offered by the U.S. National Intelligence Council, which highlighted a number of emerging technologies in its quadrennial Global Trends 2040: A More Contested World report published in March 2021. Their

future landscape is awash with yet a different set:

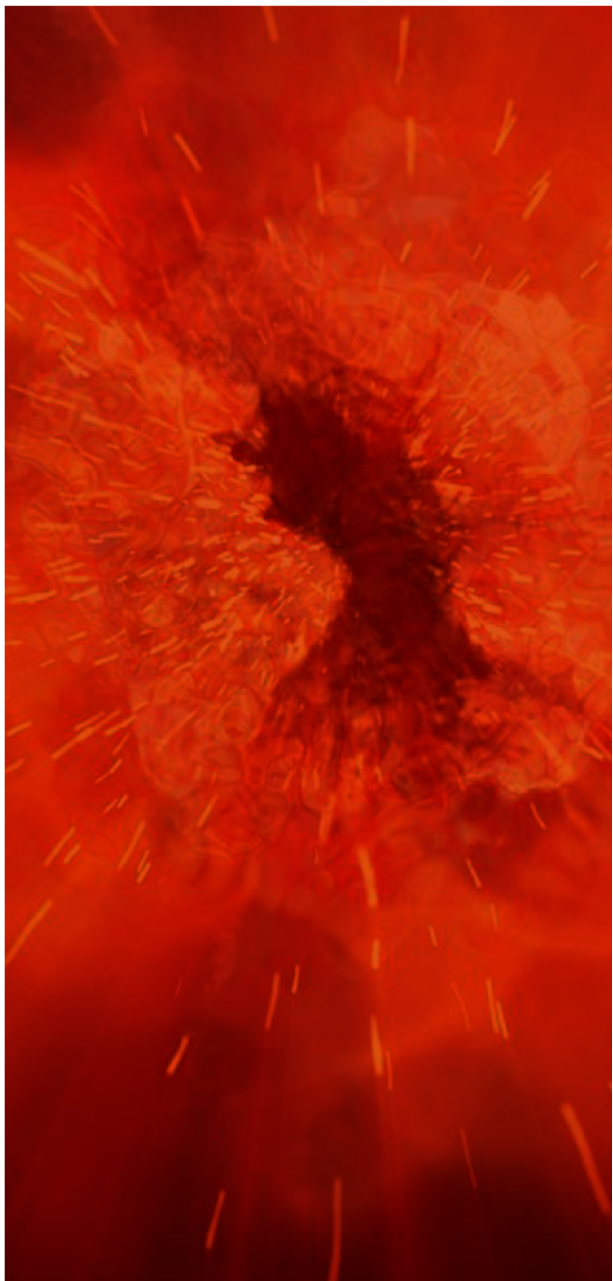
- **Robotics,**
- **the Internet of Things,**
- **AI,**
- **Virtual Reality,**
- **Advanced Computing,**
- **New Materials, and**
- **Human-Machine Interfaces, to name just a few.**⁶

Finally, the U.S. White House published its own list of “Critical and Emerging Technology” affecting national security in February 2022. This long list includes:

- **Advanced Computing,**
- **Advanced Engineering Materials,**
- **Advanced Gas Turbine Engine Technologies,**
- **Advanced Manufacturing,**
- **Advanced and Networked Sensing and Signature Management,**
- **Advanced Nuclear Energy Technologies,**
- **Artificial Intelligence,**
- **Autonomous Systems and Robotics,**
- **Biotechnologies,**
- **Communication and Networking Technologies,**
- **Directed Energy,**
- **Financial Technologies,**
- **Human-Machine Interfaces,**
- **Hypersonics,**
- **Networked Sensors and Sensing,**
- **Quantum Information Technologies,**

- **Renewable Energy Generation and Storage,**
- **Semiconductors and Microelectronics, and**
- **Space Technologies and Systems.**⁷

There are many similarities between these lists (and others), but also some important differences.



For the purposes of this report, we only chose EDTs that have the capacity to increase the effectiveness or lethality of WMDs. They are listed below in alphabetical order and not necessarily in terms of importance:

- **Advanced Computing (including supercomputing, edge computing, new architectures, big data, and sentient data),**
- **Advanced manufacturing,**
- **Artificial Intelligence (including human-machine teaming),**
- **Autonomous Robotics,**
- **Biotechnologies (including synthetic biology, or “synbio”),**
- **Cyber,**
- **The Internet-of-Things (especially relating to government or municipal IOT for infrastructure),**
- **Hypersonics, and**
- **Quantum Information Technologies.**

When EDTs are mentioned throughout this report, we are referring to one or more of the technologies on this list. Refer to Appendix 1 for a brief explanation of the EDTs with their respective current “state of the state”

WMD EFFECTS

International law conclusively defines WMDs. In this report, we do not suggest that this definition be modified at this time. Instead, during the workshop, we explored what it would take, by a combination of EDTs, to create an effect comparable to a WMD.

Using Hiroshima and Nagasaki as the standard by which to measure the effects, we arrived at three unique features of a (nuclear) WMD, described directly below:

- **Shock-and-awe.** The spectacle of instantaneous and near-total mass destruction of a city or other target.
- **Horrific, catastrophic losses.** Horrific both in how they died and how many died in the moments after detonation.
- **Long-term effects.** This refers to radiation poisoning and fallout (medical long-term impacts for individuals), but also applies to the cumulative effects and generational trauma of suffering from a WMD.

Given these factors, the question presented to workshop participants was whether EDTs paired with each other or traditional kinetic weapons (i.e., anything but a WMD) could achieve a similar level of destruction, fear, and long-term destruction

6 The National Intelligence Council, *Global Trends 2040 - A More Contested World*, 54-65.

7 Fast Track Action Subcommittee on Critical and Emerging Technologies, *Critical and Emerging Technologies List Update*.

DETERRENCE

To understand the problem of this report's central research question, it's necessary to understand the concept of deterrence. One definition of deterrence is a "strategy to prevent a target from taking an action that the deterrer finds undesirable through manipulating the target's perception of the costs, benefits, and risks of cooperating versus defecting." ⁸

As an example, while early military thinkers considered it approvingly in the context of strategy, it wasn't until the Cold War that a mix of conventional deterrence and nuclear deterrence took center stage. NATO is an alliance of nuclear power countries and non-nuclear powers, expressly designed to deter the Soviet Union from a conventional invasion of Europe. Nuclear deterrence was the "sword" of NATO deterrence, but conventional deterrence was the "shield".

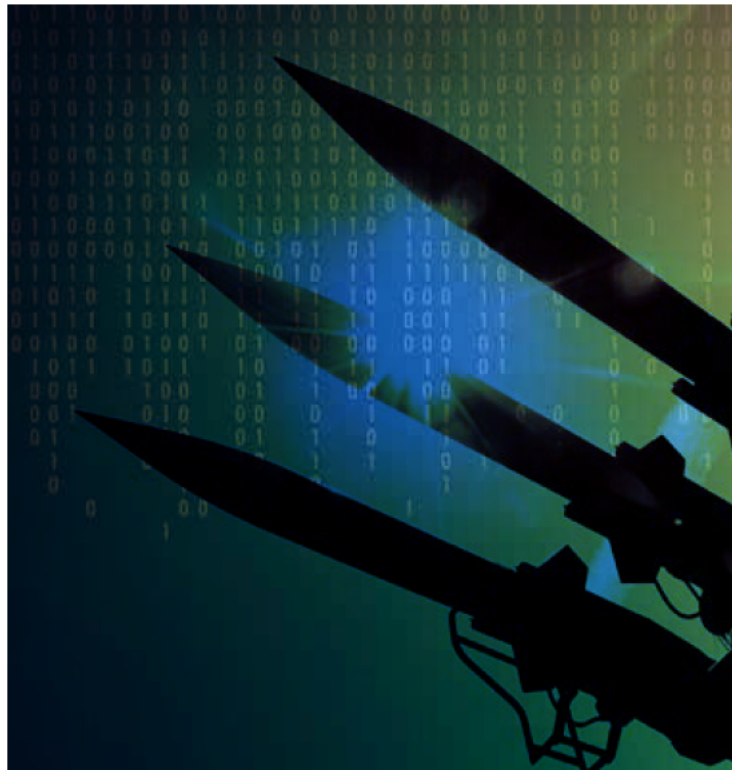
The history and theory of deterrence is too comprehensive to address here, but we can draw lessons from the Cold War that are still relevant in a future of EDTs. Below, we list six primary lessons learned from related historical events:

1. **Context and perception are critical.** Motives are not always what they initially appear to be, and each side sees through its own lens. The act of "signaling" is important for deterrence strategies because the aim of the action is to shape an adversary's perception and to get them to behave in a certain way. In order to understand and control what you are signaling, you need to understand how adversaries view those signals. This requires we read signals and events in the light of an adversary's social, cultural, economic, cognitive, and political environment. Throughout the Cold War, each side told itself a story about their strategic situation and needs. Understanding an adversary's story requires an understanding of the context in which it is written and told.
2. **"Know your enemy".** In the Cold War, we thought we knew who "The Communists" were and based all strategies around that single perception. The U.S. spent considerable resources and lost a great deal of global respect by supplying troops and money to imperialist and anti-communist dictators around the world. This did not help the U.S. cause, nor did it serve those locals who were caught in the crossfire. In fact, these actions damaged stability worldwide. It took the U.S. many years to figure out that the Chinese communists had different interests and perspectives than Moscow, which in turn artificially limited our efforts to create stability for decades to come. Not "knowing the enemy" was one dominant factor in the failures in Korea, Vietnam, Iraq,

and Afghanistan while creating a disconnect between political and military strategies. One of the best strategic moves we can now make is to be hyper prepared for several potential scenarios and outcomes. For instance, understanding China deeply will be critical for us in the coming years, (e.g., China thinks about nuclear weapons and strategy very differently than the U.S. does).

3. **Learn from the past *with nuance*.** History isn't a script, it's an epic set of interacting patterns. We can learn a lot by following how past actions have unfolded, but we need to think of this less as a rote lesson and more as a kind of intellectual fitness exercise. We need to learn from the mistakes of the past. Understanding the way human beings have interacted during times of crisis (and peace) teaches us what general things to look for. Healthy observation and pattern analysis helps us think in non-habitual ways, so we may anticipate the future in a realistic way. The following are three examples that illustrate how we have, in a way, sabotaged ourselves due to limited thinking:

1. Nation states tend to plan for the last war that they have engaged in. For instance, for decades U.S. strategy was fixated on the shock of Pearl Harbor; therefore, nearly all they planned for during those decades was a massive sneak attack from a totalitarian regime obsessed with destroying the west.
2. The lessons of the Cold War cannot be easily abstracted. Putin is "riding the wave" like the one Hitler "rode" in the late 1930s. It would be a mistake, however, to cast him in a role, even that of Stalin, which only fits a little better.
3. We've learned to wield the idea of nuclear weapons, but it's not entirely clear what we would do if presented with the choice to initiate nuclear war. Leaders often respond to the existential threat of nuclear weapons in unexpected ways. Eisenhower leveraged nuclear weapons to compensate for a conventional "draw-down". Kennedy was prepared to press the button over West Berlin. Nixon played "madman". Reagan was almost fanatically committed to nuclear abolition.



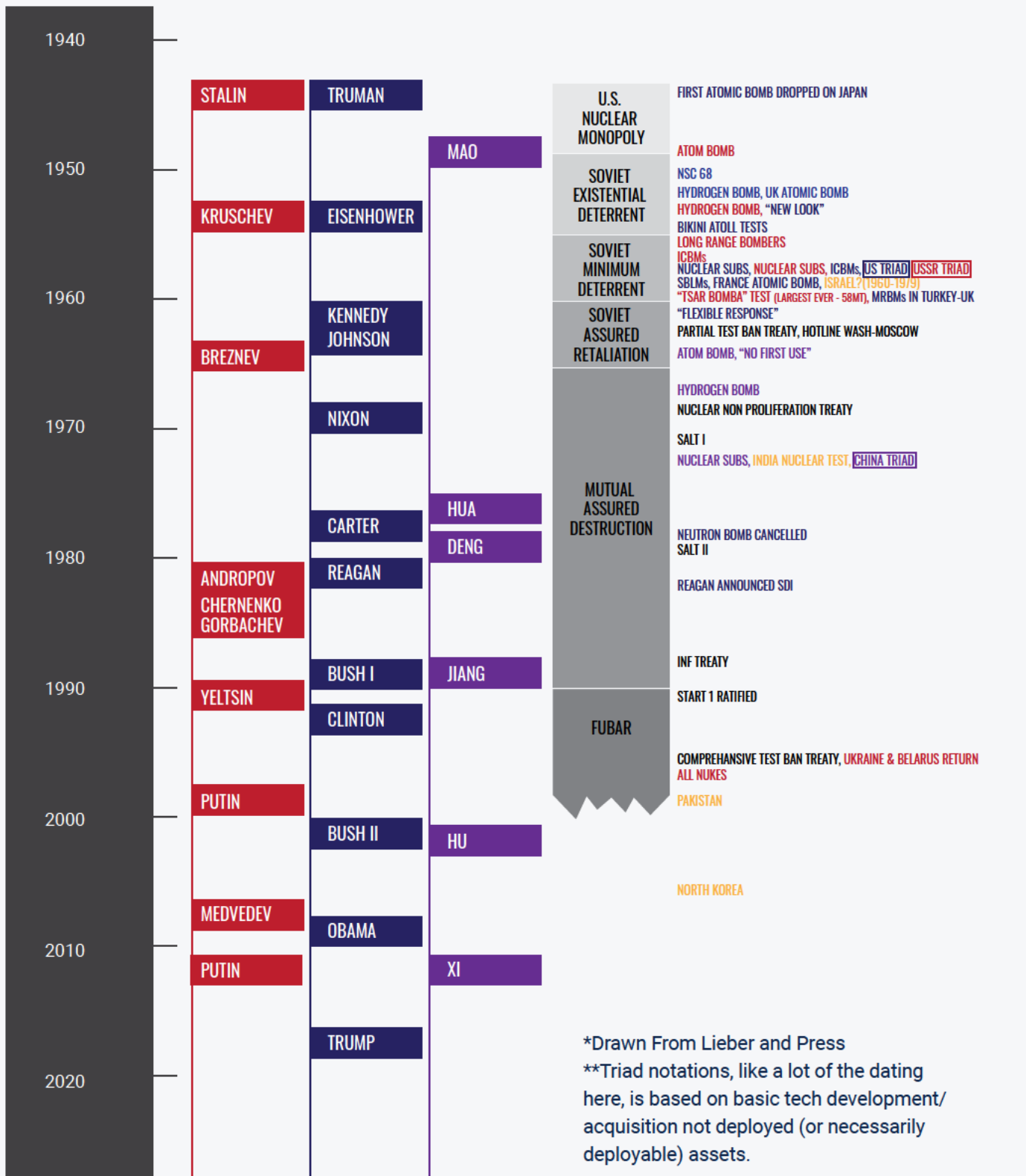
4. **It's easy to get sidetracked by a strategic plan.** The concept of developing a nuclear strategic plan is a problem and puzzle that has been worked on by generations of smart, capable people. The U.S. government has spent billions of dollars on strategic plans for global nuclear war over the course of decades. Many aspects of these projects have amounted to little more than mental gymnastics and theoretical games because we don't have concrete data to test nuclear theories against. Many plans have not been executable. The communication of the plans themselves is often unclear with inconsistent and faulty "command and control". Theoretical thinking can take plans only so far and has a tendency to abstract things, like culture, geopolitical context, domestic politics, and finance in a way that obfuscates and distorts reality. Another thing to note is that if a strategic plan appears to be too logical and perfect, it should throw up a warning flag. This is mostly because it is difficult or impossible to test the plan against the abstractions of culture, etc. While it seems logical to focus all efforts on planning for the worst, as was the case with both the U.S. and USSR throughout the Cold War, a deceptively narrow focus tends to weaken strategic flexibility. The value should remain in the action of planning, not the actual plan.



5. **Complicated, seemingly stable systems can collapse with harsh speed.** The U.S. was not prepared for the collapse of the Soviet Union. As a result, we ended up fostering conditions of economic chaos like those in Weimar Germany. As the Soviet Union collapsed, the U.S. never envisioned, and thus had no plan to, contain the political and economic shrapnel that resulted. One emerging threat was the proliferation and control of nuclear material and delivery systems that occupied U.S. strategy for an extreme length of time after the collapse.
6. **People don't want to use nuclear weapons.** The fact that nuclear weapons have not been used in war since 1945 is actually quite surprising. Nuclear weapons have been threatened for deterrence or coercive purposes and used once before there was stable nuclear deterrence to compel an end to a world war. This marks a distinct difference from using the threat of nuclear weapons for coercion short of war. Given the many close calls, both accidental and strategic, it's reasonable to call it a miracle that we have avoided general nuclear war to date.



COLD WAR TIMELINE





INTEGRATED DETERRENCE

Integrated deterrence is the current change in focus for the Department of Defense (DoD) deterrence strategy. The U.S. Secretary of Defense explicitly calls out integrated deterrence as the way forward for the Indo-Pacific area, with the goal of signaling to China and its allies that the U.S. and its allies will have technological and operational overmatch. Secretary Austin describes, “What we need is the right mix of technology, operational concepts and capabilities — all woven together and networked in a way that is so credible, flexible and so formidable that it will give any adversary pause. We need to create advantages for us and dilemmas for them.”⁹

Deterrence activities are integrated across all instruments of national power, including diplomatic, military, informational, and economic. Calculating deterrence will no longer be a one-to-one matching of nuclear weapons or a buildup of conventional forces. Instead, it will be the ability of allies and partners with common values to quickly respond to international threat that makes integrated deterrence a many-to-one strategy against adversaries. In testimony to the Senate Armed Services Committee in 2021, U.S. Pacific Fleet commander, Admiral John Aquilino, discussed deterring China from invading Taiwan as a primary objective for the Indo-Pacific region. He said, “Those forces combined with the international community, with our allies and

partners...would position us very strongly for the deterrence required.”¹⁰

The key ingredients of integrated deterrence are unity with allies who combine their available national strengths (such as: inter-service integration between land, sea, air, space, and cyberspace) as well as superior strategy, which pushes the boundaries of technology’s use to provide deterrence against grey zone aggression.

Furthermore, cyber’s role in integrated deterrence will be much more profound than during the Cold War. Cyber operations “are at their best not when they are designed to create an effect in a moment in time, but instead when they are part of a larger strategy of obfuscation, deception, and sabotage.”¹¹ Often, cyber effects are temporary and the damage they inflict can be reversible. This dynamic gives policy makers options to lower tensions when adversaries deescalate or be more aggressive when indicators of increased escalation are observed.

In fact, activities within cyberspace have demonstrated how NATO and partners might develop better integrated deterrence. In July 2021, the European Union, NATO, and the United Kingdom joined the United States in exposing the malicious cyber activities of People’s Republic of China and its attacks on Microsoft Exchange systems.¹² Allies have also supported the United States’ Cyber Command in conducting over a dozen “hunt-forward” operations against “adversary operations

and cyber vulnerabilities on their networks.”

13

In a White House summary of the strategy, they state that “We will drive initiatives that reinforce deterrence and counter coercion, such as opposing efforts to alter territorial boundaries or undermine the rights of sovereign nations at sea.”¹⁴ In the future, these deterrent initiatives will be joint, multi-domain, as well as synchronized with allies, and integrated across instruments of national power.

NORTH ATLANTIC TREATY

The North Atlantic Treaty is the foundational document of NATO, which was formed to implement signatories’ intentions “to safeguard the freedom, common heritage and civilization of the peoples, founded on the principles of democracy, individual liberty and the rule of law.”¹⁵ Ratified in April 1949 by the twelve original members of NATO and signatories, the treaty contains 14 articles, three of which are most relevant to this report. Outlined below are excerpts from and interpretations of these articles:

Article 3: “In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means

of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.”

Interpretation: This is seen within NATO as a mandate for member states to increase their resilience in the face of natural disasters, humanitarian crises, and armed attacks. In 2016, the alliance adopted seven baseline requirements against which member states can measure their level of preparedness. These requirements include: contingency plans for continuity-of-government and energy supplies; maintaining the integrity of borders in the face of uncontrolled movement of people; and resilient food, water, health, communications, and transportation systems – all to ensure NATO forces and civilian services are able to effectively respond during a crisis.

Article 4: “The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.”

Interpretation: Invoked only seven times in the alliance’s history, most recently following Russia’s invasion of Ukraine, this article is seen as the diplomatic precursor

9 Lopez, C. Todd, *Defense Secretary Says “Integrated Deterrence” Is Cornerstone of U.S. Defense*.

10 Shelbourne, Mallory, *Military Takeover of Taiwan Is Top Concern for INDOPACOM Nominee Aquilino*.

11 Loneragan, Erica, and Jacquelyn Schneider, *Cyber Challenges for the New National Defense Strategy*.

12 The White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China*.

13 Williams, Brad D, *CYBERCOM Has Conducted “Hunt-Forward” Ops in 14 Countries, Deputy Says*.

14 The White House, *Indo-Pacific Strategy of the United States*, 12

15 North Atlantic Treaty Organization (NATO), *The North Atlantic Treaty*

to mobilizing NATO forces during a crisis or emergency. In practice, it means one or more members bringing an issue of concern to the North Atlantic Council, will result in political consultations that may or may not lead to a joint decision or action by the alliance as a whole. Any decision requires consensus among all NATO members.

Article 5: “The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all, and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.”

Interpretation: This most famous article of the treaty has been invoked only once, following the attacks of 9/11. Article 5 is the heart of the alliance, assuring members will come to the military aid of their counterparts in the event of any attack, but what constitutes an Article 5 violation is not so clear in an era of disinformation, cyberwarfare, “little green men,” and now EDTs.

It is also important to note that an “attack” does not necessarily have to be a kinetic attack in the traditional sense to trigger

Article 5, provided the attack reaches the level of an armed attack.¹⁶ This is ultimately a political decision based on the consensus of NATO members. NATO has repeatedly affirmed that Article 5 extends to cyberspace, and at the NATO 2021 summit in Brussel, it amended this to clarify that the accumulation of cyber incidents could warrant Article 5. At the same time, the alliance has maintained strategic ambiguity about the precise conditions under which Article 5 might be triggered.¹⁷





16 Upeniece, *Conditions for the legal commencement of an armed attack.*

17 Lonergan and Moller, *NATO's Credibility Is on the Line with its Cyber Defense Pledge. That's a Bad Idea.*



FINDINGS

INTRODUCTION

The primary data of this report comes from dozens of subject matter expert interviews and multiple threat futures, and was generated in a series of workshops in March 2022. Afterwards, a team of analysts conducted a post-analysis to identify patterns and clusters. With a focus on the central research question, six main categories or “threat spaces” emerged from the analysis.

In this Findings section, we describe all six “threat spaces” within two separate categories that encompass two different focus areas.

The first three “threat spaces” focus on nuclear WMDs and how EDTs will increase their effectiveness and lethality. These threats explored how EDTs may accelerate the escalation of geopolitical conflicts, “lower the bar” for the use of nuclear weapons despite longstanding taboos, and how they might afford insider threats an outsized impact on the global security landscape.

The second three “threat spaces” have a focus on how EDTs might be combined with each other to attack critical infrastructure, producing a “WMD effect” without resorting to the use of traditional WMDs. This might in turn lead to “long-game” attacks on civilian infrastructure or systems, such as energy grids or agriculture. A combined assault has the capacity to eschew mass casualties from WMDs in favor of nearly imperceptible attacks that degrade a target’s integrity, eventually equaling the long-term effects of a traditional WMD attack.

FOCUS AREA 1: EDTs Effects on Traditional WMDs

Finding #1: Geopolitical Conflict Escalation

EDTs initiate, facilitate, and escalate existing geopolitical conflicts, increasing the risk of general conflict and the use of WMDs.

The advent of nuclear weapons, followed by a growing Soviet arsenal, led to the adoption of “escalation theory” in the 1960s intended to understand, predict, and strategize how a localized crisis between state actors might trigger a cascade of events leading to a general conflagration. EDTs accelerate, complicate, and scramble these classical models of escalation and deterrence.

In 1962, RAND strategist, Herman Kahn, developed a 16-¹⁸ (later 44-) step escalation ladder¹⁹, which mapped out the conditional shows of force, acts of violence, and confrontations leading to an “all-out” war. Crucial to Kahn’s model is the importance of both context and thresholds. Successful de-escalation depends on opposing actors’ mutual ability to perceive and interpret each other’s motives and intentions — without risking runaway escalation. Relatedly, escalating crises never proceed smoothly or inevitably from one rung to the next, but are tripped up at critical thresholds that act as firebreaks

on decision-making.²⁰ During and since the Cold War, WMDs acted as the ultimate firebreak, which even the Korean War or Cuban Missile Crisis could not cross.

EDTs short-circuit Kahn’s and others’ models in several respects. They scramble contexts through the use of AI and other rapid detection- and decision-making technologies that may obfuscate or deliberately mislead opposing plans and intentions. They can be used after an initial provocation to misdirect and misinform, creating strategic ambiguity, while running the risk of escalation through misattribution. These risks are amplified by non-state actors’ enhanced capabilities. For them, EDTs potentially carry more “bang for the buck” than either WMDs or conventional weapons when it comes to effects versus cost and complexity.

There are numerous EDTs that rely on AI in some form. Examples show up in many forms, such as an autonomous drone swarm deployed by a state actor or terrorist organization; a hacked civilian infrastructure leading to self-crashing cars; or a compromised NC3 system. Instances such as these run the risk of escalation through their sheer speed, lack of human oversight, and confusion. Unsupervised AI systems threaten to overwhelm human decision-makers’ OODA loops. Specifically, their ability to “observe, orient, decide, and act” in response to adversarial moves, while

¹⁸ Kahn, *Thinking About the Unthinkable*. 185.

¹⁹ Davis and Stan, *Concepts and Models of Escalation*

²⁰ Kreps, S. Schneider, J., *Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics*

remaining opaque to human judgement. These in turn create overwhelming pressure to “trust the system”. Contrast this with the case of Soviet Lt. Col. Stanislav Petrov, whose snap decision in 1983 to disregard a launch detection by a malfunctioning early-warning system, may have averted nuclear war.²¹

Future leaders like Petrov may not have the ability to intervene in a world of highly automated, autonomous, and interconnected systems. For example, in one of the 2040 scenarios created for this report, an enterprising German researcher unwittingly penetrates sensitive systems related to China’s Social Credit System. His intrusion is interpreted by Chinese AI as a state-sponsored attack, automatically triggering retaliation against Germany’s energy infrastructure. This in turn leads to consultation among NATO allies as to whether the incursion rises to the level of invoking Article 5. In no case do humans enter the loop until after autonomous systems’ moves and countermoves had created and escalated a crisis.

Some well-meaning actors might trigger a crisis of misattribution unknowingly. While other malicious state- and non-state actors will do so intentionally, perhaps in concert with the use of other EDTs or even WMDs. Using emerging technologies, such as generative AIs (e.g. deep fakes; GPT-3; DALL-E 2) nested within next-generation social media networks, actors will find it increasingly cost effective to

create confusion at scale, while the rapid deployment of countermeasures will only grow more time-consuming and difficult. As a result, EDTs are a recipe for escalation.

Finding #2: Lowering the Bar

EDTs will “lower the bar” for using WMDs.

One reason the nuclear WMD threshold hasn’t been crossed since Nagasaki may be the “nuclear taboo”²², a normative stigma powerful enough to “stay the hand” of even the most rational strategist. Other WMDs also carry taboos about their use, however, these taboos may be weaker and only elicit condemnation or outsized reactive policy responses. Conventional weapons and EDTs don’t carry the same stigma as WMDs. This is probably because the policies governing EDTs are not mature or widely agreed upon across international bodies. Societies also rarely understand the cause and effect of their weaponization. For instance, they do not fully understand how extensively a weaponized EDT can damage or disrupt normal life, whereas nuclear explosions produce glaring destructive outcomes.

EDTs risk facilitating and accelerating the crossing of escalation thresholds, and threaten to lower the bar for the deployment of WMDs. This is partly due to the expanding pool of potential participants to include non-state actors and others who have never lived in the shadow of WMDs or ever had reason to consider the nuclear taboo within their planning cycle.

For example, in one such scenario from Threatcasting participants, members of Boko Haram, supplied with sarin gas by Russia in a proxy struggle with NATO, deploys a swarm of camouflaged autonomous drones to disperse the nerve agent across Lagos. This action kills hundreds of thousands of people and results in millions of refugees fleeing to Europe. As a local proxy, Boko Haram makes what they believe to be an accurate assumption that the traditional deterrent of force on their operations by NATO is mitigated by both Russia's support and the threat of a rapidly escalating humanitarian crisis. Combining EDTs such as robotics, AI, and mimetic camouflage enhance the potential efficacy of WMDs. It also places them within reach of non-state actors whose acceptance of escalation insulates them from typical deterrence.

For state actors, the risk is the opposite. Attacking with EDTs may create a rung on the escalation ladder that trumps the nuclear taboo. In such a case, the presence of EDTs and/or WMDs on both sides might heighten tensions and lead to a situation in which one decides to either strike first or escalate with EDTs. This in turn, runs the risk of the perpetrator being met or counter-attacked with overwhelming force with seemingly no other choice than to use a nuclear WMD

Finding #3: New Insider Threats

EDTs will enable, embolden, and amplify both old and new insider threats.

The use of EDTs will introduce new vulnerabilities and produce disproportionate effects from insider threats with widely varying behavior. The intentions and effect of insiders can only be detected and modeled with difficulty. EDTs will amplify their roles as vectors, enablers, and unwitting accomplices in an unpredictably exponential manner, propelling them to the global stage and enabling them to affect "geopolitical dominos".

In contrast to adversaries with clearly stated or observable intentions, insider threats may arise from things such as a sense of injustice, personal desperation, ignorance, or even unknowing manipulation. In addition, they may serve as deployment-and-delivery systems, such as ferrying drones and other-weaponized robotics through criminal logistics networks. In another scenario, one might imagine them doubling as unsuspecting carriers of personalized synthetic bioweapons that target world leaders or other persons-of-interest.²³ They could conceivably act as radicalized "lone wolves" abusing access to dual-use EDTs, such as cyber or quantum.

In yet another Threatcasting scenario, a Seoul National University quantum

21 Chan, Stanislav Petrov, *Soviet Officer Who Helped Avert Nuclear War, Is Dead at 77*.

22 Tannenwald, Nina, *The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use*, 433–68.

23 Hessel, Goodman, and Kotler, *Hacking the President's DNA*.

researcher deceives their naïve assistant into hacking North Korean nuclear command, control, and communications systems (NC3) under the guise of a simulation. This researcher's mentor, a North Korean refugee whose family was purged and persecuted by the regime, consequently, obtains control of the DPRK's nuclear arsenal and retargets one of its weapons to detonate above Pyongyang. The surviving leadership, understandably assuming a first strike by the West, orders nuclear retaliation against Seoul and a hypersonic attack on Seattle. The first salvo's death toll is in the millions.

In addition to the above-mentioned scenarios, EDTs can be used to create or augment insider threats themselves. Cyber and AI manipulation are projected to be applied to compromise the mental health and security of personnel with access to critical systems. In this manner, EDTs can be combined to create novel pathways for escalation. Combatting such threats will require a comprehensive approach that moves beyond traditional vigilance and deterrence to encompass mental health, domestic disinformation, and corruption.

FOCUS AREA 2: EDTs and Combined EDTs That Bring About WMD Effects

Finding #4: WMD Effects

Combining EDTs will create a "WMD effect" – novel attacks with the hallmarks of WMDs although not typically classified as such.

One reason the nuclear taboo exists is that

even in the absence of further escalation, nuclear WMDs create effects that are different in kind as well as magnitude. The horrific spectacle of instantaneous destruction, mass death, and chaotic disruption...ranging from millennia of contamination to nuclear winter²⁴ ...places WMDs in another category altogether. However, by pairing or combining multiple EDTs, such as robotics, AI and autonomous systems, quantum, and hypersonics, state and non-state actors can achieve the speed, scale, and destruction of WMDs without crossing the nuclear threshold. As noted above, this will simultaneously escalate and lower the bar for the actual use of WMDs.

While unlikely to replicate the full scope of WMD effects in a single attack, novel pairings of EDTs will succeed in achieving both immediate shock-and-awe and long-term degradation of the target's strategic resource. For example, cyber and quantum weapons might be deployed against civilian energy or transportation infrastructure to instigate a local or regional attack with global shocks. Examples include such attacks on Ukraine's power grid in 2015 and 2016 (and allegedly in 2022)²⁵, or conceivably hacking personal vehicles to create widespread collisions, chaos, and deaths. More subtle attacks on critical social systems, such as healthcare, agriculture, finance, industry, and politics will have less visibility, but potentially more profound effects over time.

Such strategic combinations of EDTs will embolden actors who would otherwise be unwilling or unable to employ WMDs and risk nuclear escalation. Workshop participants proposed a future scenario in which China pairs a hypersonic show-of-force — sinking a pair of its own vessels in international waters off the coast of the United States with an unprecedented autonomous drone strike on Taiwan’s military infrastructure. In this case, with its now-established hypersonic capabilities acting as a deterrent against naval intervention, China’s swarm destroys the island’s defenses in startling fashion, achieving a *fait accompli* backed by the implicit threat of nuclear escalation.

This participant’s Threatcasting scenario is notable for the absence of conventional forces. Rather than attacking the island with amphibious landings and capital ships, EDTs are capable of attaining strategic goals on their own. In this way, combining EDTs offers more “bang-for-the-buck” for non-state actors traditionally denied access to WMDs and states that will find them more cost effective than nuclear options.

Finding #5: Destabilizing Critical Infrastructure

EDTs will be deployed to destabilize complex systems to achieve the long-term effects of a WMD.

The initial shock and destruction of combined EDT attacks will be accompanied by more pervasive and insidious efforts

to achieve the long-term degradation of the opponent’s strategic resources and capabilities. In turn, reducing its will and capacity to fight. The primary targets of these incursions will be the complex and interdependent systems undergirding nations and the international rules-based order. Examples of these systems are energy and infrastructure; healthcare; agriculture and food production; trade and finance; industry and raw materials; and other institutions essential to a functioning society.

The second- and third-order effects of these repeated attacks will be an erosion of trust in the affected systems and institutions with the ability to create crises, unrest, and strategic paralysis. In the absence of an antagonist through an explicit attack with WMDs, the effects of these EDTs will be internalized, politicized, and increasingly intractable amidst domestic disputes. Breakdowns of social systems will manifest unpredictably through public disorder, infrastructure failures, domestic terrorism, and eventually large-scale effects that will present themselves as collapsing birth rates, rising deaths, and a steady decline in life expectancy.

This type of destabilization will be accelerated through outright misinformation and manipulation. Once again, EDTs such as cyber and AI will be instrumental in both maximizing the

efficacy and concealing perpetrators responsible for attacks. An early example of this dynamic is the 2016 “Heart of Texas” protest secretly fomented by the Russian Internet Research Agency through opposing Facebook groups used to galvanize interest.²⁶ With recent rapid advances in generative AI, it is not difficult to imagine how EDTs combined with insider threats will continue to corrode public trust and potentially spur populations to war.

Finding #6: The Long Game

EDTs enable a new “long game” approach to creating WMD effects over time.

The greatest threat posed by EDTs compared to WMDs is their imperceptibility. Through the creative and deliberate use of EDTs to attack, destabilize, and undermine critical systems, political will, and social cohesion, opponents might achieve the strategic effects of a WMD without their target’s population even being aware they were the victims of an attack.

In addition to economic inequality and political polarization, EDTs might also be employed to explicitly attack entire populations without detection. The COVID-19 pandemic has underscored how even a virus with a low positivity and death-rate has the propensity to trigger global upheaval. This is seen through broken supply chains, closed borders, and a long-term public health crisis. Future advances in virology and genetics raise the possibility

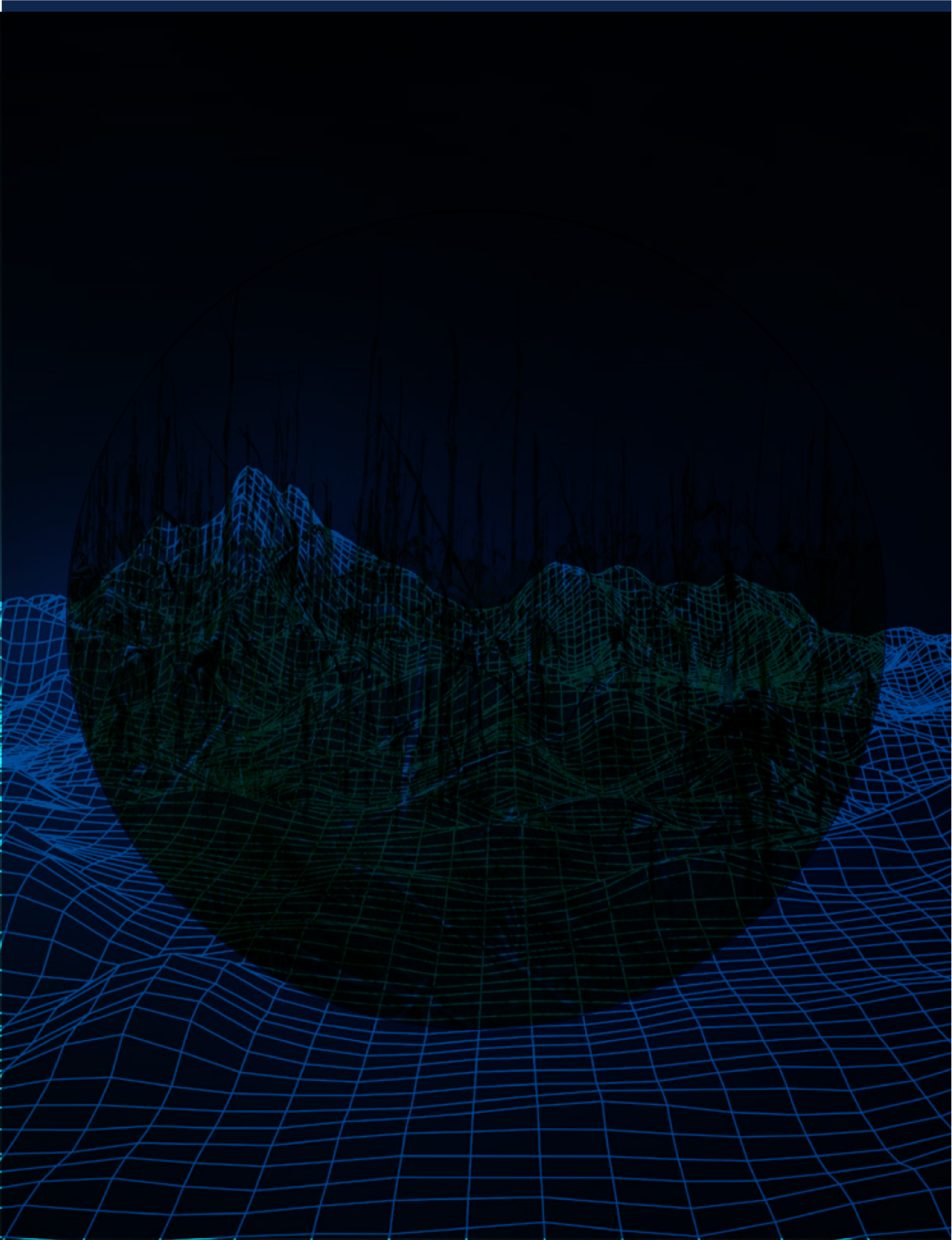
of deliberately infecting and debilitating populations over years – to include indirect effects in rising healthcare costs, declining productivity, skewed dependency ratios, and other phenomena with dire consequences.

Another domain of concern is agriculture and the environment, which are both currently under stress in the West due to climate change. The global struggle by the U.S., China, and regional powers to secure a global food supply has already produced allegations of agricultural espionage, intellectual property theft, and genetic tampering.²⁷ For example, imagine a modified virus attacks wheat or soybeans rather than human beings, which would trigger crop blights, soaring food prices, and societal breakdown. This could, with relative ease, be fueled by information EDTs.

The implications of this imperceptible “long-game” attack vector are sobering. EDTs may simulate the effects of WMDs without detection, and unlike the detonation of a nuclear missile above a city, society itself might be the attack surface

²⁶ Riedl, Strover, Cao, Choi, Limov, and Schnell, *Reverse-engineering political protest: the Russian Internet Research Agency in the Heart of Texas*.

²⁷ Genoways, *Corn Wars*.





BACKCASTING

FLAGS

FLAGS DEFINITION

The Threatcasting methodology maps out possible and potential threats 10 years in the future and attempts to identify the flags or indicators that serve as signals that a specific threat future is underway. Sometimes referred to as “signals”, these flags can give an early warning that a possible future threat is in progress or beginning to form. Often, flags are sequential with less apparent precursors and with more alarming flags over the horizon.

EDT AND WMD THREAT INDICATOR AREAS:

The data from the workshop provided three cluster groups of flags that will signal the progression and development of EDTs. These groupings apply to all six findings listed earlier in the report. Listed below, they are a place for organizations to begin to monitor the progression of EDTs:

1. EDT Technical Progress and Break Throughs,
2. Geopolitical, Cultural, and Business Trends, and
3. Early Use, Rehearsals, and Attacks.

In this section, we provide details for each flag grouping as well as examples pulled from the workshop data. These indicators are not complete or definitive; however, are a place to start. An organization should investigate its own monitoring activities and use the following as a beginning guide



EDT Technical Progresses and Break Throughs

Monitoring the progress and potential technological break throughs for emerging disruptive technologies is the primary landscape to monitor. It will be important to monitor the progress of multiple EDTs at the same time, as it is the combination of multiple EDTs that have the potential to increase the lethality of traditional WMDs or WMD-like effects. Below, we provide an overview of the most critical EDTs to monitor as well as where to find and how to monitor them.

Review of Critical EDT(s)

- Advanced computing - including supercomputing, edge computing, new architectures, big data, and sentient data;
- Advanced manufacturing;
- Artificial Intelligence - including human-machine teaming;
- Autonomous Robotics;
- Biotechnologies - including synthetic biology;
- Cyber;
- Industrial IoT - especially governmental or municipal IOT for infrastructure;
- Hypersonics; and
- Quantum Information Technologies.

Where to Look and How to Monitor

The indicators will occur in multiple areas, including academic research, private industry, corporate research and product offerings, as well as government and military research. The first two areas, academia and private industry, should be generally simple to monitor, while the remaining areas are likely more difficult to identify because of the efforts of nation states and militaries to protect their secrets

Academia and Private Industry

It may seem like monitoring the progress and development of EDTs is a daunting task. However, there are specific key areas that can be observed to give an organization early and robust indicators on the development and use of EDTs.

A large part of the early-stage experimentation and development of EDTs will occur in academic and research institutions. A key metric to observe in this area are publications, presentations, and public lectures. Academia follows the motto of “publish or perish”, which pushes university researchers, professors, and students to produce a constant

stream of papers and lectures, which publicize the successes and progress of their work. An academic search and monitoring of these areas focused on EDT development will provide insight into their progress.

Additionally, academic research is often funded by government and foundation grants. These calls for research proposals, funding award notifications, progress reports, and final results are publicly searchable and trackable.

Private industry research and development is not as transparent. The strategic value of the development of EDTs will be seen as a corporate secret. However, progress can be tracked through patent filings, early product offerings, and support staffing.

Patents are typically filed five to ten years before the technology or breakthrough is ready for public use. Patents need to be filed with various global patent offices. These patent documents outline, in detail, the progression and uses for the technology requiring a patent. The constant monitoring of patent filings for specific EDT technologies will give a long-range window into the development progress as well as who is submitting patents in these areas.

A more short-term indicator of the progress of EDT development can be found in publicly available product descriptions and early-stage marketing. The information may be about a hardware or software offering with an overview of the technology and its capabilities. Like patents, the product offering will also indicate which organizations and companies are participating in the development.

Finally, hiring notices or support staffing can give a mid-term indicator of EDT technology development in industry. For an organization to bring an EDT to market, they need a specific set of expertise and skills associated with the technology. Monitoring calls for applicants around key EDT terms will give organizations a clear indicator that an EDT is being prepared for release.

Government and Military

Successful monitoring of the EDT development progress within government and military organizations will also be key. It is anticipated that some of these EDTs will be designed and developed within various security environments, and therefore, not discussed in public forums.

For instance, the U.S. Intelligence Community scientific and technical intelligence

organizations will need to use a comprehensive set of ways to capture intelligence, including:

- Signals Intelligence (SIGINT) - to include Communications Intelligence (COMINT), Electronic Intelligence (ELINT), Technical ELINT (TechELINT) and Foreign Instrumentation Signals (FISINT);
- Human Intelligence (HUMINT);
- Geospatial Intelligence (GEOINT) - to include Imagery (IMINT) and geospatial information;
- Measurement and Signature Intelligence (MASINT) - to include such things as thermal infrared heating imaging, acoustic signatures, and seismic data;
- Open Source Intelligence (OSINT) - to include foreign open source acquisitions (gray literature) and patents;
- Foreign Materiel exploitation - to develop knowledge on the capabilities and performance of foreign weapon systems, including chemical and biological weapons, future weapons concepts, and developing technologies that have potential military applications; and
- Counter-Intelligence (CI) Activities – to determine foreign collection priorities in order to secure U.S. knowledge. This includes CI agents gathering foreign technology development knowledge to augment U.S. technology development efforts.

In addition, these organizations need to use horizon scanning for early detection and assessment of emerging technologies and threats. Identifying intelligence analytics will integrate data with behavioral, biometrics, forensics, and other associated identity signatures. This will in turn further identify key academics, engineers, and scientists developing new technologies and weapons. Organizations will need to model and simulate weapons capabilities and performance based on their understanding of technology developments. Assessing what technologies are needed based on the expected future operating environment will be important as well as conducting doctrinal gap analysis to determine required weapon systems and technologies. Additionally, there will be a need to track technology proliferation, production, and manufacturing capabilities. These organizations will work with U.S. technology and weapons developers to understand both obstacles to development and capability results.

There is a need to prioritize intelligence collection on the most stressing threats to U.S. national interests, key adversaries, competitors, and technology innovators. Functional areas of concern include WMDs and cyber. Priorities for further intelligence collection will also be based on identified knowledge gaps in the intelligence communities' analysis.

Example Indicators of EDT Progress

These are some of the indicators (flags) on the technological progression and breakthroughs associated with the development of EDTs. They were taken from the Threatcasting workshop and then synthesized and clustered by the analysts. Additional indicators from current and projected trends for each ET area are also included. The results indicate that organizations should monitor:

- Advances in **ADVANCED COMPUTING**, such as:
 - Advances in virtual, augmented, and mixed reality (AR/VR/MR) systems to the point that they are fully immersive with limited technological barriers.
 - Supercomputing, which reaches speeds of hundreds or thousands of exaflops (50 or more times faster than the fastest supercomputers of 2022)²⁸ and pushes artificial intelligence and scientific discoveries into new territories.
 - Overly restrictive domestic (United States and European Union) regulations on supercomputing, high-performance computing, and AI applications that allow unregulated markets to have an advantage.
 - A reduction in funding from federal sources that slows the development of national advanced computing objectives.
 - The corporate appetite for more data, which makes industry a better source of intelligence than national intelligence systems.
- A broad range of **SYNTHETIC BIOLOGY ADVANCES**, including:
 - Further development to perfect synthetic biology and virus creation, lowering the complexity and cost.
 - Pairings of synthetic biology technology with other EDTs.²⁹
 - Synthetic biology specificity that improves microtargeting at the individual level.
 - The expansion and deepening of the connection between *cyber technologies* and synthetic biology.
 - The expansion and deepening of the connection between *nanotechnology* and synthetic biology.
 - Government approval for greater genetically modified organism use in food, medicine, and other industrial applications (e.g., plastics, clothing)
- Advances in **ADVANCED MANUFACTURING**, including:
 - The creation of new materials capable of being 3D printed.
 - The development of chemical weapons that can withstand explosive kinetic delivery systems.
 - Nanotechnology that enables objects to harvest energy from their environment.
 - “Self-healing” or self-assembling materials through nano-scale engineering

- Expansion of **ARTIFICIAL INTELLIGENCE** adoption and applications, including:
 - The development of Adversarial AI applications that attack other AI and cybersecurity systems.
 - Widespread adoption of synthetically fabricated video, audio, and pictures (so-called Deep Fakes) with cheap (“as-a-service” model) or open-source tool sets.
 - AI education and career opportunities that reach a tipping point and pushes China into a position of global dominance within the field of AI.
 - Widespread adoption of AI-generated “social credit” programs that reward or restrict citizen behavior.
 - Demonstration of human-out-of-the-loop decision making for nuclear command and control systems.
- Advances in the development and use of **AUTONOMOUS TECHNOLOGIES**, such as:
 - Progress and implementation of autonomous systems for uses in supply chain and shipping.
 - Industrialization of an autonomous credit ranking system that is ready for deployment and use in the market.
 - Further development of perfect drone swarms’ autonomous behavior and navigation, especially in a GPS-denied environment.
 - Novel weaponized applications of drones in all environments (e.g., air, land, sea, space), including the use of drones to deliver WMDs³⁰.
 - Standardization of counter-drone policies and technologies³¹ that provide malicious users knowledge of legal and technical boundaries to push against.
 - Expansion and regulation of the drone insurance and liability industry.
 - Demonstration and doctrinal employment of drone swarms in combat situations³².

28 Department of Energy, *U.S. Department of Energy and Cray to Deliver Record-Setting Frontier Supercomputer at ORNL*.

29 Scown and Keasling, *Sustainable Manufacturing with Synthetic Biology*, 304–7.

30 Kallenborn and Bleek, *Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons*, 5–6.

31 Garrett-Glaser, *Drone Security Near Airports a ‘Wicked Problem,’ Says FAA*.

32 Kallenborn, *The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It* and Hambling, *What Are Drone Swarms And Why Does Every Military Suddenly Want One?*

- Within the **CYBER DOMAIN**:
 - Global clarity on where the “red lines” exist for malicious cyber activities and the nations that are following through on promises to defend those red line intrusions.
 - Further development of regulations and policies about data collection, storage, processing, privacy, and ownership.
 - The deepening of connections between cyber technologies and other EDTs (i.e., through connectivity, speed, data, security, or risk management frameworks).
- **INDUSTRIAL IOT**:
 - A greater coupling of IIoT sensors with edge computing and localized, automated decision-making processes (e.g., artificial intelligence or modeling).³³
 - Increased automated decision making on the controls and outputs of IIoT rather than just the sensor data (e.g., adding water treatment chemicals, opening and/or closing of dam flood gates, and other cyber physical systems).
- **HYPERSONICS**:
 - Construction of advanced testing facilities that can support wind tunnels beyond Mach 10.
 - Multiple successful tests of hypersonic glide vehicles prior to proof of fielding.
 - Russian or Chinese hypersonic technology sales to other nations.
 - Development of hypersonic weapon detection and interdiction technologies.
 - Progress towards international standards for hypersonic weapon controls.
 - Continued advancement of on-board, edge computing technologies that improve targeting response once a hypersonic vehicle is launched.
- **QUANTUM TECHNOLOGY**:
 - Further development of quantum technologies to the point where solutions and activities are observable, such as proof of breaking sophisticated encryptions.
 - Improvement in sourcing materials for manufacturing quantum computers, such as improved purity, reduced defects, and reduced “noise” in materials.³⁴
 - Scalable technical advances, such as error correction techniques, room temperature capable quantum computers, and chip miniaturization advances.
 - Increased investment in logistics and financing of quantum development.

Projected Threat Curves for EDT Development

As an organization monitors the progression and development of EDT technologies, it is possible to identify key changes and influences in the development cycle that can disrupt, slow down, and/or hasten the deployment of the EDT. Additionally, it is important to identify if the EDT has a dual-use³⁵, and where the technology has both a positive effect and negative impact. For example, nuclear technology is a dual-use technology. It can be used for good, as is the case in developing power plants, but can also be used to harm the population, as is the case in developing nuclear weapons. In addition, by recognizing the influences and dual-use capabilities of EDTs, organizations can make informed decisions about their response to the development of EDT technologies.

The following is a breakdown of the threat curves for each EDT:

Advanced computing, which includes supercomputing, edge computing, new architectures, big data, and sentient data. Influences on advanced computing mainly come from academia and private industry. Over the decades, as advanced computing has become more normalized into global society, it can be seen as an “environment” or condition from which many opportunities and threats can arise. The market success and capitalization of these technologies drive their development - with strategic shocks or innovations coming from new products and the application of advanced computing to new uses. Developing advanced computing within government and military applications, especially those that are government funded, can advance or hasten the speed of its development.

The disruptions in this area can come from the two areas of business or implementation failures and government regulation. Just as industry supplies the capital to fund the development of this technology, the failure of the technology to be monetized can disrupt its development. As industrial use of advanced computing solutions grows and turns into “big business”, there is a physical point where governments will step in to regulate the technology. This can slow down the development of the technology and place restrictions on its use – normally, for the safety of consumers.

33 Boyes, Hallaq, Cunningham, and Watson, The Industrial Internet of Things (IIoT), 1–12.

34 Leon, Itoh, Kim, Mehta, Northup, Paik, Palmer, Samarth, Sangtawesin, and Steuerma, Materials Challenges and Opportunities for Quantum Computing Hardware

35 Dual-Use Definition: Traditionally, the term “dual-use” is used to describe items that can be used for both military and civilian applications. Throughout this report, we use the term to describe EDTs that can be used for both good and bad purposes

Advanced computing is a strong dual-use technology, as it provides a platform for business and social benefit, while at the same time, providing a platform for crime, information warfare, infrastructure attacks, and civil unrest. However, over the decades, advanced computing has become woven into the fabric of 21st-century life, making it hard to completely disrupt its progression.

Advanced manufacturing. Advanced manufacturing is mainly driven by industry, as its advances are integrated into existing business processes. This is also true for militaries that have similar use cases to incorporate its applications. The advances in its development are tied directly to monetization efforts and industry investment.

Disruption as well as strategic shocks or innovations are generally rooted in materials science, especially in the case of 3D printing. Advances in the materials used to manufacture different industrial and biological products have both a great positive and negative influence. Currently, government regulation is not a large factor in the development of this technology. As the industries around the technology grow, however; it may be possible to imagine government restriction in this area.

Advanced manufacturing is also a dual-use technology. However, it has mostly positive uses with industrial applications. The main negative purpose it's used for is in the manufacturing of weapons, especially nuclear and biological weapon systems. This could also change the nature of

weapon systems in that weapon systems could be designed and built as "individuals" for a specific purpose, and therefore would be harder to build systems to defeat them. It would also allow for individuals or less powerful states an opportunity to build advanced systems, as they would just need to steal the CAD drawings, and use advanced manufacturing methods to create the weapon systems.



Artificial Intelligence (which includes human-machine teaming) and Autonomous Robotics.

Artificial Intelligence (AI) and Autonomous Robotics are two separate EDTs that share similar threat curves. They are different in that AI is solely a software platform, where autonomous systems are a mix of software and hardware.

Industry, academia, and government have all driven the research and growth of these technologies. Early-stage development was typically funded by the government in research labs and academia. When the technology had sufficiently progressed, it was transitioned to industry for commercialization. Currently, the majority of investments for these technologies occurs in industry. Like most industry-driven technologies, commercialization and monetization are key drivers for success. However, these technologies are unique in that they serve a role outside of exclusive consumer usage.

Another fact, however, is that AI and robotics are and will be continuously used in military and defense environments. This will give them a more stable development pipeline as opposed to those developed as purely commercial technologies. Because military and defense use cases are different than industry, basic R&D will continue in military and academic settings until they have progressed to the point where they can be transitioned to industry. For instance, consider AI development within a bell curve. Most of the use cases that

industry design fall within the 80% center of the curve, where a lot of data exists, and the impact of errors may cause a company to lose market share. In contrast, the use cases for defense applications exist within the lower percentage tails of the bell curve. Here the data is sparse, the environment is actively contested and congested, and the results of errors can lead to unintended deaths. Similarly, defense use cases for autonomous robotics differ from general society needs. Therefore, R&D for these EDTs will occur in a multitude of different locations.

Disruptors to these AI technologies fall into the two categories of regulation and innovation. Currently, both technologies are being investigated and debated about where and when they need to be regulated. This regulation could limit development and slow progress. Secondly, there are currently significant technological hurdles that need to be crossed in order for EDT innovation to advance.

During the last two decades, AI has also progressed mainly in one specific area, called Machine Learning (ML). These advances have been commercialized and are being used successfully in multiple industries. However, there is a debate as to whether advances are still possible in AI.³⁶ The debate revolves around the types of AI that might be the next frontier for innovation. DARPA describes that we are currently in the 2nd wave of AI (statistical learning) and is investing in high-risk, high-payoff projects associated with the 3rd

wave of AI (contextual adaptation).³⁷ In this wave, the systems will think and reason much more like humans and be able to understand what is going on contextually, based off of only a handful of data points or examples.

Robotics has also seen explosive growth in the past two decades. This has been driven by the cost of computational power dropping as well as the physical hardware (e.g., servers, motors, sensors, batteries, etc.), which has been dropping in cost as well. Continued advancement of this EDT will depend on a long string of breakthroughs and advances in the machinery, sensors, connectivity, and supply chain as well as cost, business models, and materials. The slowdown of any one or more other of these could disrupt the large-scale development of the EDT.

Both EDTs have a strong dual-use. They can be used for a wide range of industrial and civil activities, while at the same time, being weaponized.

Biotechnologies, including synthetic biology. Industry, academia, and government have all driven the research and growth of biotechnologies. Early-stage development was typically funded by the government in research labs and academia. When the technology sufficiently progresses, it's then supposed to transition to industry for commercialization. This transition has not happened yet. The majority of investment for biotechnology, therefore, is now occurring in government

and academia.

Disrupters to these technologies fall within the two categories of regulation and innovation. Currently, this EDT is being investigated and debated as to where, when, and how they need to be regulated. The scrutiny of biotech is high because many aspects of it touch living organisms, the production of living organisms, and at times, the altering of human DNA. If regulated, it could limit development and slow down progress significantly. It is important to note that this debate and possible regulation does not apply to all countries.³⁸ The COVID-19 global pandemic has also made the world more aware of the consequences of a biological or viral threat. Furthermore, the hesitancy or misunderstanding of the field could disrupt its progress.

In addition, there are significant technological hurdles that need to be crossed to allow this EDT to advance. These hurdles center around commercialization and realistic applications areas.

Biotech has a strong dual-use. It can be used for a wide range of industrial and civil activities, while at the same time, be weaponized.

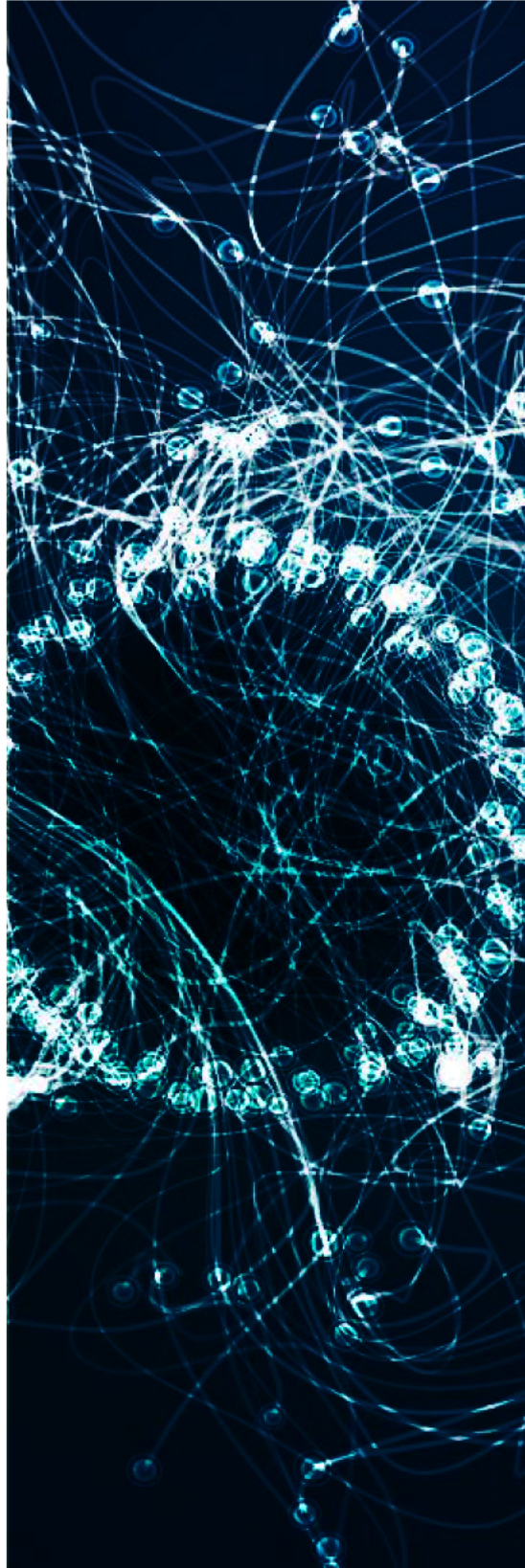
Cyber. The main influences on cyber are from government, academia, and industry. Over the last decades, cyber has been used as a broad term, focused more on cyber-attacks and cyber defense or cybersecurity. As the field has become normalized into global society, it is now also seen as an

“environment” or condition from which many threats have arisen. Government and military applications, especially development that is government funded, can advance or hasten the speed of the development. The market success and capitalization of cyber has been focused on defense and security with strategic shocks or innovations coming from new products and applications.


The disruptions in this area can come from increasing regulation, currently focused on infrastructure and the use of cyber as an offensive weapon. Because of its implications to national and international security, this EDT is likely to be intensely watched and debated over for the foreseeable future.

Cyber is a strong dual-use technology that provides a platform for crime, information warfare, infrastructure attacks, and civil unrest, while also providing an industrial and government opportunity for defense and security. Unlike other EDTs included in this report, it is the intent behind the deployment of cyber capabilities that determines if the use is positive or negative. This dichotomy of intent is similar to the difference between the use of a nuclear warhead or a nuclear power plant. The science and technology are the same, but the intent and desired effects are in complete opposition with each other.

However, over the decades, cyber has become woven into the fabric of 21st-century life, making it difficult to disrupt its progression.



37 Defense Advanced Research Projects Agency (DARPA), *DARPA Perspective on AI*.
38 Inglesby, Ciceroa, Riversa, and Zhangb, *Biosafety and biosecurity in the era of synthetic biology*.



Industrial Internet of Things (IIoT), especially, government or municipal IIoT incorporated into critical infrastructure. Industrial IoT is mainly driven by industry, as its advances are integrated into existing business processes. The advances in its development are tied directly to monetization efforts and industry investment. Additionally, most recommendations for the incorporation of this EDT into military or defense forces have an almost identical use-case model to industry use cases.

Currently, there are few signs that this EDT will see government regulation since it has been seamlessly merged with existing industrial applications. Often in the U.S., the decision to regulate is strongly correlated to the application's industry versus the technology on its own merits. However, this may not apply if the EDT is used in applications where public funds are invested or civilian lives could be endangered by its misuse or failure. The use of public funds and the possible danger to the lives of citizens differentiates this use of IoT from IIoT. With these two factors, there is a high probability that it will be more heavily regulated, which in turn is likely to slow its progress and adoption.

Innovation is a second area that could disrupt IIoT, such as with robotics. In the past ten years, we have seen the wide commercial adoption of IoT, and the drop in cost of computational power and physical hardware (e.g., microphones, sensors, batteries, etc.). Continued advancement of this EDT will depend likewise on a long string of breakthroughs and advances in the machinery, sensors, connectivity as well as supply chain, cost, business models, and materials. The slowdown of any one or more of these could disrupt the large-scale development of the overall EDT.

IIoT has a weak dual-use. Most of the applications are positive and are compatible with current business activities. However, the increased use and adoption of this EDT does make it a platform that can be hacked or hijacked to be used for an attack. This means that the IIoT devices themselves are not being weaponized, but the interconnectivity of them provides new attack opportunities for adversaries.

Hypersonics. Of all the EDTs, hypersonics is the most unique. Their development and advances are so expensive that they are almost entirely driven by government and military applications. Technology innovation hurdles and global regulations will be the key disruptors, as hypersonic missile systems have a direct effect on national and global security. In particular, hypersonic and glide-boost systems compress the decision-making timelines and emphasize first-strike doctrine that may lead to crisis instability.³⁹

Hypersonics are also unique to this list because they are a weak dual-use technology because their main purpose is to be used as a weapon. The U.S. has made it a point to research hypersonics with the intent to arm them with conventional warheads, but China and Russia have not ruled out the nuclear option for their programs.⁴⁰

Quantum Information Technologies. Quantum technologies are still in the theoretical and early-stage of development. Currently, the potential of this EDT far outweighs the reality of its effects. However, if perfected, it will have a considerable impact on encryption, digital security systems, and the advancement of new materials productions. The influences and development of this EDT are taking place across all sectors, including academic, government, and industry. There are considerable efforts underway in scientific research and development of potential counter measures to mitigate the effects of Quantum technologies.

The disruption to quantum information technologies is considerable and mainly technical and scientific in nature. To bring this EDT into broad use, significant scientific advances need to be made in the field of quantum mechanics, materials design, technological design, and software development. If any one of these scientific categories is not developed to the degree it needs to be, then the progress of the EDT will be disrupted.

Because of the massive effect that Quantum technologies could have, regulators are sure to keep a close watch on developments and breakthroughs. When the technology does become viable, considerable regulation will disrupt its progress.

This EDT has a strong dual-use. Currently, most parties are focusing on the potential ill effects, as mentioned above. However, it could also bring about significant advances in materials technology and new materials creation.

³⁹ Sayler and Woolf, Defense Primer: Hypersonic Boost-Glide Weapons.

⁴⁰ Kunertova and Dominika, Weaponized and Overhyped: Hypersonic Technology.

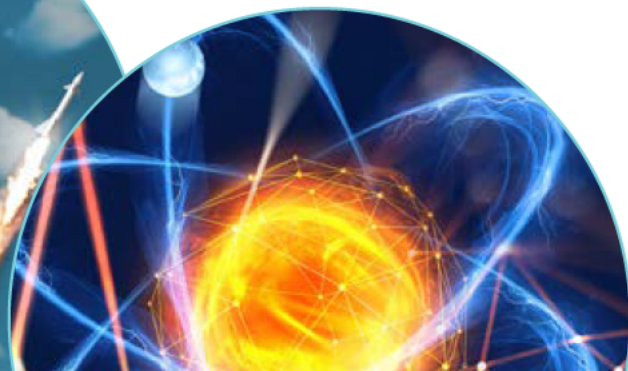
2.

Geopolitical, Cultural, and Business Trends

The threat futures in this report depend heavily on the conditions in which the EDTs are deployed to increase the lethality of WMDs or produce WMD-like effects. This scope is beyond the monitoring of the technological progress of EDTs, and the conditions or trends will span geopolitical, cultural, and business applications.

If an organization monitors these indicators, it will improve their ability to see the developing conditions that contribute to the increased probability and susceptibility to threat futures. The grouping of these trends is broken into the following three areas, since the places and people needing to be monitored will be different.

- **Geopolitical** - refers to nation states, local and national governments, and militaries, etc.
- **Cultural** - refers to civilians, the general public, and media opinions, etc.
- **Industry** - refers to the private sector, corporations, industry, and trade associations, etc.



Geopolitical

The global geopolitical stage can provide organizations with a clear environment to monitor changes, shifts, and advances. Observing the political shifts of different countries as well as their approach to international relations will be key indicators. These changes will lay the foundation for an atmosphere that will make the six findings and possible threats more likely to occur.

Organizations should monitor:

- The escalation and rise of tensions and loyalties between state vs. federal entities.
- The increase of local and national government affiliations with separatist movements.
- Evidence of the weakening of treaties with specific examples of treaties being violated.
- Several nuclear issues, including broad international calls for denuclearization, evidence of the sale of fissile material to individuals (not states) as well as the emergence of the development and availability of tactical nukes.
- Changing policies and behaviors indicating an acceptance of the usage of limited tactical nuclear devices.
- The escalation of minority suppression under the guise of terrorist threats.
- Increased economic and cultural divisions within societies.
- The exclusion of specific groups or countries from the national or international conflict resolution process.
- If the U.S. intelligence community is slow to adapt to EDTs.

Cultural

As the geopolitical landscape can indicate actions and attitudes of governments, so too can cultural shifts indicate changes in public sentiment. These shifts can be subtle at first or initially documented by the media or special interest groups. Changes in culture influence both geopolitical and business sectors as well. They can have a powerful effect on the atmosphere and norms around the use of WMDs and EDTs.

Organizations should monitor:

- Changing consumer opinions and behaviors, such as when they begin to express a high trust in autonomous systems decision-making, show signs of blind faith in security and security breaches. Other signs include when they exhibit dependence on poorly secured IoT or a willingness to divulge personal health info, and/or when political divides cause them to ignore science-based findings and facts in favor of identity politics.
- Purposeful use of disinformation on the general public to confuse and fuel tensions.
- An increasing wealth gap that creates two specific sets of protections for consumers, such as those who can afford to pay for protection and security and those who cannot. Yet other indicators would be the rich moving to fortified, off-grid rural safe havens

and/or if increasing urbanization continues to strain infrastructure for those who cannot afford to move.

- If technological improvements, proliferation, and advances of EDTs and adjacent technologies begin to accelerate disintegration of society. This condition begins with many assumptions, namely causality and correlation issues. Is it even possible that disinformation could degrade society? Think of social media platforms competing for ad revenue and your personal data; news outlets “soapboxing” to be heard over the volume of “news”; and the connectivity of phones having immediate access to all these information flows. Each system contributes, but more research is needed to show causation.
- The increase of mental health challenges, which raises questions around rational actor theory. Extreme stress or an overwhelming sense of helplessness, such as death of family, existential threats, etc. may change someone’s reservation to kill or may push them to extreme action



Industry

Much of the development of EDTs will occur in the private sector. Monitoring the business or industrial sector for changes and advances can provide key indicators along with the technical progression outlined above. Because industry will drive the development and adoption of EDTs, the adoption and use in normalized business operations will be a key indicator of future adoption by consumers and governments.

55

Organizations should monitor:

- The increased commercialization of space.
- The increasing of business practices that are dependent on automation at scale. Examples of this are greater AI involvement in supply chain operations and when industry begins to express, exhibit, and implement a dependence on poorly secured IoT.
- If industry begins to express, exhibit, and implement a blind faith in security and the belief that security breaches are a one-off.
- The evidence of increasing capital investments in synthetic biology startups.
- Technology services and platforms, such as GitHub that are given access to and begin to monetize genetic data and models.

3.

Early Use, Rehearsals, and Attacks

The final grouping of indicators combines EDT technological progress and breakthroughs with the geopolitical, cultural, and business trends that set conditions for WMD effects. This grouping of indicators illustrates a ramping up of severity over time. Organizations need to track EDT early use, rehearsals, and attacks. A description of each is provided below:

- **Early Use.** Early use does not necessarily indicate adversarial action, but simply the adoption of technology or any of the practices above that improve the conditions for an adversary's advantage.
- **Rehearsals.** Rehearsals are generally tests that take place to prove that a strategy works, to show a technology can achieve a specific effect, and/or to show others that an attack is possible.
- **Attacks.** Attacks are the final step as an indicator. These early attacks may have a greater magnitude than a rehearsal, but they are early enough for organizations to mitigate their effects and prepare for recovery

Early Use

The early use of EDTs is the first step that will indicate that an EDT threat is likely to occur. For many organizations when early use is detected, activities shift from disruption of the threat to mitigation tactics. In other words, the threat cannot be stopped and now its effects must be lessened.

Organizations should monitor:

- Early use and adoption of Autonomous Systems, such as connecting NC3 to automated decision making; the acceptance and use of greater AI involvement in intrusion detection; and the publication of doctrinal changes in how these systems can be used.
- Evidence and increased instances of adversarial hackers given leeway to do what the official state cannot.
- The emergence and evidence of multination coordinated cyber attacks.

Rehearsals

Rehearsals are the next step in the indicator process that can show an organization that an EDT attack is imminent. In many attacks, adversaries will practice or rehearse their attacks. They are, in fact, testing the attack(s) to make sure that it is possible and to refine their approach. These activities have been seen in military⁴¹, law enforcement and terrorist attacks⁴². Often these rehearsals take place in environments with less security or oversight, so that the test will go undetected.

Organizations should monitor:

- Evidence of groups practicing and perfecting new EDT tactics in simulations.
- The practice of maneuvers and the development of hardware and software technologies to perfect the effective use of drone swarms.
- The practice of tactics and the perfecting of hardware and software technologies to combine synthetic biology, virus creation, and/or nanotechnology.
- Early evidence of individuals and/or groups manipulating the IoT outside of a laboratory or research setting.
- Evidence of the use of camouflaging technologies to mask EDT delivery systems.

57



Attacks

Attacks are the final step in the monitoring process. When early-stage attacks are discovered, organizations can move from disruption and mitigation tactics to recovery plans. Because the evidence of attacks is highly evident, this report does not focus in detail on them. However, the specific attacks below could indicate that a larger attack is imminent. These attacks are typically just the first step in a long and more destructive chain of events.

Organizations should monitor:

- Evidence of attacks on critical electricity and water infrastructure.
- Evidence that NC3 upgrades can be hacked from outside the system.
- Observed changes in the norms of greater nuclear use that shift to using tactical nuclear weapons.

⁴¹ Sevastopulo, *US defence chief warns of China 'rehearsals' for attack on Taiwan*.

⁴² JCAT, *Counter Terrorism Guide*.

MOTIVATIONS

A significant part of creating an effects-based model is to imagine a threat actor and what things need to be in place for them to be successful. Participants in Threatcasting workshops spend considerable effort thinking about what variables enable the actor's success. Main factors to consider are the motivations, values, and objectives that drive the threat actor's actions.

WMDs have a potential for death and chaos on such a massive scale, that they have been front-and-center in U.S. national defense narratives since the time of President Eisenhower, and were formalized in the U.S. National Security Strategy of 1990.⁴³ Articulating the influence of WMDs on national strategy, the Council on Strategic Risks suggests, "Beyond the use of nuclear weapons for deterrence, it is clear that some actors likely consider using WMD in order to capitalize on their disproportionate psychological effects and for their significant advantage of mass publicity."⁴⁴ In other words, NATO members must consider the advantages provided to the wielder of WMDs. They need to identify the motivations of those with access to nuclear weapons who often differ significantly than those "home-brewed" synbio agents in a makeshift lab. It is to the latter type of actor that we consider having different motivations.

We assessed that threat actors fall into three general categories with a fourth category that describes certain conditional states that take the threat further. Each actor category contains several broad motivators. These actor categories and respective motivators are discussed below.

⁴³ Bajema, *Definitions Matter: The Role of WMD in Shaping U.S. National Security Strategy*.

⁴⁴ Ibid.

⁴⁵ Nesser, *Single Actor Terrorism*



SINGLE ACTOR, WITHOUT SUPPORT

In our data, the single actor category (usually described as an individual) tends to use EDTs to create WMD-like effects without external support or funding from a nation state. Often, insider knowledge or access is critical to single-actor success. Petter Nesser, writing in *Perspectives on Terrorism*, illustrates current terrorism literature in separating “lone wolf” terrorists acting on their own from solo terrorists acting with support from a larger group.⁴⁵

These actors are motivated to use EDTs or WMDs for three reasons. The first is for personal financial gain, where the actor may use the threat of WMDs to coerce a ransom or payment from their victims. Additional motivators explored by our models in this category include criminal theft or fraud, getting the “life one deserves”, or even a seeming altruistic goal of providing for one’s family.

The second motivator for single actors is to vindicate an ideological slight or a personal grudge. For example, one of the Threatcasting teams imagined how Dr. Kaitlen Barnes uses an experimental form of a topical chemical weapon transfer to kill her less-qualified, yet more rapidly promoted male coworkers. Dr. Barnes then takes the weapon global to further liberate women from male oppression. Likewise, another Threatcasting team considered the driving effect of a hyper-intelligent quantum researcher who sought additional recognition for his unappreciated research.

“Dude”, the name of the story’s threat actor, sells his quantum research to a terrorist organization via the dark web and assists them in assembling a 3D-printed nuclear device that detonates at a New York City New Year’s Eve party.

The third motivation was unknown. Namely, some single actors become threats for unknown reasons, or may even be tricked into enabling a WMD-like effect. This category is the most terrifying, simply because there are fewer indicators preceding the WMD event. Threats in this category may be enabled by misinformation or disinformation, and the actor might even believe they are correcting the natural order, according to their beliefs.

NON-NATION STATE GROUP

The next category of actors are non-nation state groups. We distinguish these from single actors without additional support because the models separated out several individuals with interconnected responsibilities. However, the non-nation state group includes incidents of violence or terrorism conducted by a single actor, but with explicit support from a group, which is often associated as a named terrorist organization, religious cult, or ideological faction. Our distinction is that non-nation state groups also are not misled or tricked into their attacks, and normally take their actions because of financial or ideological reasons. Actual examples outside of the Threatcasting simulations include the 2017 suicide bombings in Mogadishu, Somalia, that killed at least 588 people, injured

another 300; and the 1995 Aum Shinrikyo sarin gas attack on the Tokyo subway that injured over 5500 people.⁴⁶

Over the next decade, non-nation state groups will continue to employ EDTs to make their attacks more lethal. For example, a Threatcasting team imagined hackers from Hackers of Planet Earth (HOPE) whom setup quantum relays in China to investigate how the Chinese national military command uses AI to direct their nuclear forces. In this scenario, HOPE inadvertently triggers China's AI-based detection program and escalates nuclear tensions around the world.

A different Threatcasting team visualized the impact of camouflage technologies in preserving Boko Haram's growing stockpile of AI-enabled drone swarms in the group's efforts to demonstrate their dissatisfaction with the Nigerian government's modernization plans.

STATE ACTORS

The third category of actors are clearly linked to nation states, even if that country uses a "single person" as part of their purposes. Although it is rare for a single actor to represent the interests of an entire nation, the effects-based models of Threatcasting purposefully use the story of a person experiencing the threat. The motivators for state actors are distinct from the motivators of a single actor, and include furthering offensive strategies, reacting defensively, and/or improving sovereignty, ethnic, or national superiority.

Offensive strategies are nation-state actions that indicate aggressive changes or political dominance often through coercion or threats of force. As an example, a Threatcasting team envisioned how Pakistan begins to normalize and accept the use of "miniaturized conventional physics devices" or small tactical nuclear bombs. Continuing with this scenario, Prabal, a Pakistani artillery battalion commander, receives authorization to fire one of these tactical nukes on a larger Indian force, which successfully wins the skirmish.

In a similar vein, a different Threatcasting team imagined China using multiple EDTs, including drone swarms, AI, robotic amphibious vehicles, and hypersonic weapons to rapidly seize Taiwan, and directly confront the United States' political position towards Taiwan. In this scenario, Chinese leaders declare any U.S. interference would be cross their nuclear red line.

There are several models in which the Threatcasting participants imagined state actors using EDTs to progress a position of sovereignty, ethnic, or national superiority. In these models, the state focuses inward on its own population or to neighboring countries to influence a localized or regional response.

In a model imagined by a Threatcasting team, China used advances in synthetic biology, combined with DNA collected from on-going population suppression operations in the Xinjiang Province, to

develop biological weapons that specifically targeted Uyghur phenotypes. This model illustrates the Chinese Communist Party's position on the genetic superiority of Han ancestry.

CONDITIONAL STATES

Rather than requiring a threat actor to actively become involved in creating a threat future, there are circumstances in which no actor is involved, yet the threat continues to escalate. In these situations, there is no threat actor attempting to meet a criminal, ideological, or nation-state objective. A conditional-state threat appears as an unforeseen circumstance when a combination of one or more EDTs interact together to create a WMD-like effect. A new conditional state might appear when EDTs collide with a changing environment, such as climate change. This includes natural disasters, especially a disaster that causes nuclear fallout to contaminate a wide area.

For example, a Threatcasting team imagined how many unforeseen interactions exist with current technologies and future quantum devices. In this model, China develops a quantum-based radar that is capable of detecting submarines under the water. An accidental interaction with the quantum radar technologies and nuclear material causes a U.S. submarine carrying nuclear missiles to explode. Tsunamis and long-term radioactive fallout affect millions along the coasts of Taiwan and China.



ACTIONS TO BE TAKEN

To develop responses to future threats, NATO uses a framework of “Outs”. These Outs are actions intended to out-compete adversaries. They describe aspects of strategic preparation and operational readiness to confront and defeat adversarial uses of EDTs and WMDs. The six Outs are Out-Think, Out-Excel, Out-Fight, Out-Pace, Out-Partner, and Out-Last. They frame our analysis and help us to synthesize our workshop participants’ visions for NATO actions, investments, and responses to future threats. Additionally, each of the six Outs has multiple subcategories we consistently apply across each of our six findings. Some subcategories were more relevant to a particular finding than others. Additionally, the number of recommended actions does not imply importance or priority. Each alliance member will need to consider how best to implement these recommendations individually and collectively.

OUT-THINK THE ADVERSARY

How and what should NATO and alliance members do to out-think their adversary? How can they anticipate the adversary’s plans, create awareness of their actions prior to an attack, and make faster, more effective decisions once threats are revealed? To start, members must have correct information. NATO’s mutually trained intelligence processes and personnel are critical for gathering and understanding the vast amounts of data, information, and processed intelligence needed to out-think the adversary. Our data suggests this understanding arrives from several mutually reinforcing activities, including exploratory basic and applied research, detection and sensing, data sharing, and anticipatory decision-making informed by wargames at the individual country level



1. RESEARCH AND INTELLIGENCE GATHERING.

Examples are utilizing detection and surveillance technologies along with sensemaking, data sharing, and anticipatory decision-making processes. This category includes intelligence activities which enable NATO members to explore, understand, and anticipate new threats, actors, and events in which EDTs can escalate conflicts and heighten the risk of WMDs. It includes three subcategories..

- a. **Research and anticipatory decision-making.** NATO must redefine the threat landscape around EDTs through research and anticipatory decision-making that explores potential incidents and actions related to WMDs. Broader research in this area will give NATO and members a better understanding of the possibilities and threats from EDTs. These activities should include:



- Understanding the ramifications of non-traditional, non-nation-state actors with access to WMDs or EDTs capable of producing WMD effects as well as how these alter alliance preparations and decision-making.
- Enhancing resilience by investigating vulnerabilities to attacks aimed at industrial and critical infrastructure, designed to destabilize national and international stability.
- Exploring potential benefits from human-and-machine-paired systems aimed towards halting conflict escalation and aiding in rapid decision-making during attacks.
- Investigating further potential threats from dual-use EDTs, the pairing of EDTs for WMD effects, and how such threats alter decision-making and preparation.
- Considering how the development of EDTs may shift the advantage to an adversary, and therefore change their typical posture to seize new opportunities.
- Exploring the ramifications of a nation-state or organization at odds with NATO which are achieving dominance in a specific EDT, especially those associated with decision-making and disinformation

b. Sensing and sharing. NATO can begin the sensing phase of the global development of these technologies once corresponding EDTs have been researched and defined, and their possible applications explored. The research and anticipatory decision-making (outlined above) will inform NATO about the factors to watch out for. Once the indicator of the progression and use of EDTs have been established, NATO can begin sharing this information across member organizations.

Traditionally, disruptive technologies emerge as poorly understood and marginal threats to the business practices of well-entrenched competitors. Only later, does the combination of their low costs, unforeseen uses, and new adopters prove to be troublesome. Given the dangers posed by EDTs, NATO must raise the bar on sensing the emergence and potential of new threats and technologies as well as share the information among members and institutions in time to coordinate an appropriate response. Below, we recommend actions for NATO to take in both the Sensing and Sharing categories.

i. Sensing

- Develop sensing networks and partnerships to monitor the development and progress of nascent EDTs on their path to weaponization, such as 3D-printed

explosives, biogenetics, human enhancement, and quantum, etc. Monitoring should take place in government, private industry, academic, and criminal settings.

- Monitor adversarial nation-state actors, such as China, Russia, and Iran as well as their cooperation on the development and use of EDTs.
- Expand capabilities to monitor EDT acquisition and testing by non-state actors and individual, insider threats motivated by ideology, financial gain, or other reasons.
- Develop early indicators-and-warnings (I&W) systems to watch for the weaponization of EDTs and/or their association with WMD development.

ii. Sharing

- Strengthen partnerships to monitor and exchange information regarding EDT development, testing, and associated misinformation regarding nation-state actors, non-nation-state, and/or non-traditional groups, as well as individuals' actions.
- Enhance the sharing and utilization of information and real-time analysis to create better situational awareness and security agency collaboration across member states.
- Create formats for intelligence sharing and communication that are salient, actionable, and digestible through all levels of partner countries and organizations.



2. **EXPLORATORY R&D** This refers to partnering with private industry, academia, and research institutions to guide and accelerate the development of EDTs and their countermeasures. Recommend actions for NATO are to::

- Not limit themselves to addressing EDTs as they emerge, but rather actively conceptualize, partner, and develop critically important EDTs and their countermeasures. Some EDTs, such as cyber and quantum, require more robust security measures, while others such as AI, biogenetics, and robotics will be critical for the alliance's own deterrence capabilities. Understanding the possibilities and limitations of EDTs are instrumental in predicting their evolution and countering them effectively.
- Encourage and coordinate with alliance members and organizations to draft and execute a research agenda for high-priority EDTs. Development should be pursued with both the aim of better understanding these technologies and designing effective countermeasures and actions to prevent adversarial use.
- Focus this research agenda on considering the novelty and unique features of each technology, rather than attempting to retrofit EDTs to existing doctrine and scenarios.
- Coordinate closely with partners in private industry to encourage the investment and development of critical EDTs. High priority areas for development include AI, autonomous robotics, hypersonics, biotechnologies, and quantum, etc.
- Liaise with members and partner organizations to explore rebalancing defense spending away from kinetic capabilities and toward infrastructure and capacity building in technological regulatory and enforcement bodies

3. **COLLABORATIVE WARGAMING AND PLANNING.** This refers to simulating, exercising, and considering how threats might behave as well as the anticipatory and post-event actions a NATO member might take at an individual level to disrupt, mitigate, and recover from a threat event.

The recommend action for NATO here is to conduct new wargames and similar exercises at both the alliance- and individual-member level to explore threats and events involving EDTs that may lead to conflict escalation and the use of WMDs. These events will test members' current communication and collaboration around such threats and start the development of new playbooks for countering EDTs. In these exercises, members should explore how:

- New combinations of actors, threats, cultural divisions, and EDTs create scenarios which simultaneously heighten the potential for escalation and lower the bar for WMDs. Answer the questions, what conflict thresholds are crossed more easily, and under what conditions might WMDs be conceivably used?
- Non-traditional, non-nation state, and irrational actors with access to EDTs alter traditional strategies and methods for deterrence.
- EDT attacks on critical infrastructure might produce systemic failures, and what the consequences of those failures — along with accompanying second- and third-order effects — might look like.
- NATO's steps to recover from an attack with WMDs or paired EDTs that may create WMD effects.
- EDTs enable "long game" attacks on critical infrastructure and industrial targets that might otherwise go undetected.
- Best to detect, deter, and disarm insider threats armed — knowingly or unknowingly — with EDTs. Address what safeguards, deterrence mechanisms, and civil society programs might be effective in lowering risks posed by actors who are financially desperate or ideologically radicalized.

OUT-EXCEL THE ADVERSARY

In this section, we address how and what NATO and alliance members should do to out-excel the adversary. We answer: How do they strive for excellence in development, detection, and deterrence? What research and investments should they make? What initiatives should they design? -And what actions must occur across the spectrum from peace-to-crisis-to-conflict, both simultaneously and continuously? Achieving excellence depends in part on understanding adversaries' motivations and capabilities; investing in the training, expertise, and tools necessary to counter potential threats; and developing shared infrastructure and capabilities to guide and regulate the evolution of these technologies.

- 1. DEVELOPMENTAL RESEARCH & DEVELOPMENT (R&D).** This refers to the preparation of technologies, systems, institutions, and regulations for the evolution of EDTs from exploratory R&D to full-scale production, commercialization, and weaponization.

As EDTs evolve beyond proof-of-concepts and prototypes, NATO and its members must be prepared to develop, manufacture, operate, and regulate these technologies at scale. This requires building the necessary skills, supply chain, production capabilities, and training as well as the legal and policy frameworks needed to ensure responsible use and avoidance of proliferation. With that said, recommended actions for NATO in this category are to:

- Develop new detection systems and counter-measures for biological WMDs (and dual-use medical research) aimed at both humans and agriculture, that can be paired with EDTs.
- Support research into quantum sensors and appropriate counter-measures to prevent the detection of submarines in the nuclear triad.
- Encourage investment in biodiversity through sponsorship of academic R&D and assistance in research with commercial partners.
- Develop a data protection scheme for open-source data sets used in training EDTs to prevent exploitation by adversaries and data corruption.

- 2. TRAINING AND BEST PRACTICES.** Here we mean the establishing of best practices for the detection and monitoring of EDTs, intelligence gathering, and sharing. Included with these is investing in the creation of training and research centers for educating NATO staff on the dangers of escalation and WMD effects.

Understanding EDTs' potential to transform conflict, accelerate escalation, and produce WMD effects without the actual use of WMDs will require broad investment in the research and development of new best practices for their detection and monitoring. This in turn will require NATO and its members to invest accordingly in new training and skills to instill these best practices at every level of the alliance. Doing so demands the creation of new facilities, centers of excellence, and tools to prepare NATO staff to meet these challenges. In order to accomplish this, we recommend NATO:

- Lead the development of a cross-alliance training environment for EDTs, with an emphasis on their potential to escalate conflicts and create WMD effects.
- Lead the creation of a research center to better understand the motivations of traditional adversaries, non-nation-state actors, and insider threats as well as the ramifications of their access to EDTs.
- Coordinate with members to invest in tools and establish standards and best practice for EDT detection and monitoring, intelligence gathering, and tracking development of dual-use technologies (e.g., AI).

3. PURCHASES & INVESTMENTS. In this section, we are referring to the recommendation of expenditures for the mature or nearly-mature technologies, processes, and systems needed for safeguarding critical infrastructure and systems.

One of the most dangerous aspects of EDTs is their ability to achieve long-game WMD effects with minimal warning or detection. Attacks on critical infrastructure and social systems, such as agriculture, health, and energy can lead to an overall erosion in quality of life, public trust, and ultimately political will that degrades the alliance's ability to fight. As EDTs reach maturity, NATO must invest in both their development as well as the creation of safeguards against threats from adversaries, non-traditional actors, and insider threats. Recommended investments and activities for NATO include:


- Encouraging alliance members and partner organizations to strategically invest in private industry and academia to create industrial policies that prioritize the development of critical EDTs.
- Urging members to increase investment in critical infrastructure for national and global defense. Specific emphasis should be placed on systems most vulnerable to long-game attacks, including food security and agriculture, energy, health, and democratic processes.
- Creating a biogenetic, weapon-sensing apparatus for early detection, along with established plans for mitigation and recovery in the event of an attack.

OUT-FIGHT THE ADVERSARY

How does NATO out-fight the adversary? How does it deliver deterrence, defend the integrity of the alliance, enhance security outside its members, and ensure it maintains both a decisive military advantage and political cohesion? Combatting potential threats from EDTs will require doctrinal, operational, and strategic changes to both deterrence and preparing for conflict. How should NATO expand-and-enhance its warfighting capabilities to meet adversaries armed with EDTs?

1. **CHANGE THE WAY WE FIGHT.** Here we refer to doctrinal, operational, and strategic formation changes as well as updates to ideology, communication methods, resource staging and distribution plans, and information operations. An example of this is counter-disinformation programs.

An EDTs' ability to simultaneously escalate conflicts while lowering the bar for WMD use, creates a new level of complexity when capabilities are massed. This scenario could rapidly escalate through the overwhelming creation of multiple dilemmas (both in frequency and magnitude). This in turn, would create multiple, inter-locking wicked problems resulting in decision paralysis. Additionally, non-nation-state actors armed with EDTs may create outcomes that are beyond the scope and capabilities of a traditional military alliance response. NATO should coordinate closely with members and organizations to adjust tactics in preparation for EDTs' unique capabilities by drawing on lessons from previous "Outs".



Institutional and operational resilience must be assured in order to ensure offensive capabilities can be enacted without significant repudiation. This will require NATO to further invest in:

- Expanding its information warfare capabilities to combat disinformation and create more effective cross-cultural international communication. These operations should include more time for fact-checking, validation, and attribution of activities, attacks, and consequences.
- Embracing AI-aided decision-making, keeping humans integrated in the process rather than relying on unsupervised automated systems.
- Building relationships with international, national, and local law enforcement in member nations to regulate dual-use EDTs and interdict weaponized threats by non-nation-state actors and insider threats.
- Preparing for hard-power aggression by China and/or Russia using kinetic and non-kinetic EDTs.
- Preparing for the incidental and non-traditional use of WMDs and the required, subsequent recovery efforts. Begin deploying forward defenses into densely populated areas to increase local resilience.
- Researching critical resources and reserves needed to mitigate attacks by EDTs or EDTs paired with WMDs.
- Exploring what it means to fight against non-human actors. Address what TTPs, doctrine, preparation, and educational tasks will need to be incorporated into the military and political bodies within NATO.
- Developing agile, secure, and resilient communication systems that can operate in both contested and congested data environments across alliance members. These networks should be integrated with member states.
- Determining a nation's "sacred cows" and question whether these long-standing assumptions hold true against EDTs (see sidebar for more information).

SACRED COW

A “sacred cow” is an idea, custom, or institution so strong that people believe in it without question, even when criticism is warranted. Considered central to an organization’s culture or belief system, these ideas risk becoming a critical weakness if they prevent the organization from adapting to a future environment in which the assumptions are no longer true.



Figure #2. Military Innovation?

U.S. military history is filled with “sacred cows”. A classic example in the U.S. Army is the importance of cavalry. As automatic weapons and motorized vehicles were developed simultaneously in the early 20th century, the idea of horse-drawn transportation remained so ingrained, that battlefield commanders tried at first to fix machine guns on horse-drawn carriages. The gradual transition from horses to motorized formations required a cultural and doctrinal change as much as it did a technological one.

A non-technical example of a sacred cow within the U.S. Army is the size of an infantry squad, which is the keystone of Army doctrine and operations. In 1946, after WWII, the U.S. Army reduced the size of an infantry squad from 12 to 9 personnel. However, even given the changes in the social dimension of war, technological dimension of war, and logistics in the last 75+ years, the size of the basic fighting element of the U.S. Army has not changed.⁴⁷

NATO’s world view is that of a world of nation-states operating as nation-states do. However, future threat actors within this space could be non-nation state actors including multi-national corporations. This could be another sacred cow.

⁴⁷ Hassan, *Rethinking the U.S. Army Infantry Rifle Squad*

- 2. ASSESS DETERRENCE'S ROLE WITH EDTs.** With this, we refer to activities that legitimize EDTs as a distinct category of threats and incorporating them into updated models of deterrence.

EDTs pose a particular challenge to models of deterrence designed in the 1960s for nuclear WMDs. Given they were designed to deter or de-escalate conflicts with nation-state actors, and were later updated to include non-nation-state actors who were deterred in part through non-proliferation agreements, EDTs may fall outside that particular mental construct. For example, how does one deter an unknowing insider threat who is unaware of the consequence of their actions? Can traditional deterrence theory even be modified to work with EDTs - many of which have a significant digital component?

Building off of the “Outs” in previous sections, new training and best practices for EDTs must include updated methods and thinking around deterrence. Our recommended actions for NATO here are to:

- Broaden deterrence strategies beyond nuclear WMDs to include EDTs, non-traditional actors, and insider threats as well as the consequences of paired EDTs to create WMD effects.
- Rethink deterrence in the context of a post-Ukraine invasion and geo-political conflict escalation, with a focus on preventing the emergence of a Russia-China political and economic block.
- Conduct a Table-Top Exercise (TTX) on how an Article 4- or Article 5-based response to a non-kinetic EDT attack might play out through the political and military processes of NATO



OUT-PACE THE ADVERSARY

How can NATO and its members out-pace the adversary, using new policies, processes, and technology to minimize the risks of WMD use and disrupt the adversary's decision-making process (OODA loop) in an EDT environment? This will not only require pre-emptive regulation and restrictions on EDTs, but also rethinking logistics, communications, and planning to adapt in the face of new- and emerging threats.

- 1. REGULATIONS AND POLICIES.** We refer here to the passing of laws, signing of treaties, drafting of regulations, and formulation of policies to specifically address potential threats posed by novel uses of EDTs.

Decades of nuclear arms reduction- and non-proliferation treaties, coupled with international monitoring efforts and national restrictions on the export of dual-use technologies have all been instrumental to reducing the risks of WMDs. A new generation of EDTs will require similar policies and institutions to regulate dual-use technologies, such as robotics and AI, while restricting EDTs and WMDs, such as the biological agents capable of being paired with EDTs to create WMD effects. The recommended actions for NATO are to:

- Establish a NATO-wide cybersecurity verification process for industry. NATO and its members should adopt a rating system and incentives to create a “race to the top” in cybersecurity investments.
- Establish international standards for the regulation and restriction of the use of EDTs and corresponding dual-use technologies. These standards could be modeled on current export controls and other procedures. They should also be compatible with previous recommendations (see above) to create an international detection and monitoring apparatus.
- Implement new regulations and restrictions on the import-, export- and use- of foreign (i.e., non-alliance) technologies in critical areas, such as agriculture and energy. Given the potential for long-game attacks, infrastructure in these systems must also be held to higher standards of sourcing and security, etc.
- Expand regulation of biological weapons development to further explore the potential for developing counter-measures.
- Actively engage broad swaths of the population in reshaping norms and institutions for democratic governance in the face of EDTs.

- 2. SPEED OF ACTION.** Speed of action means prioritizing events, technologies, and decision-making processes in which a rapid response is essential to maintaining a strategic and operational advantage.

Given EDTs' potential to rapidly escalate conflicts and create long-game WMD effects through attacks on infrastructure, it is incumbent on NATO to redesign its communication and supply lines to accelerate its responses to threats. NATO must expand and tighten communications between members, traditional partners, and new partners to match the sheer speed and disruption posed by EDTs. It must also reconceive "resilience" as a proactive capability in terms of how quickly NATO can meet and mitigate new threats, rather than simply have the capacity to recover from them. To accomplish this, our recommended actions for NATO are to:

- Strengthen defenses and supply lines to bring medical assistance and infrastructure to the "front lines" in the event of an attack.
- Harden supply chains and create contingency plans for EDT attacks by non-nation-state actors and long-game scenarios.
- Draw on new capabilities and investments (See: Out-Excel the Adversary) to reconceive resilience as a strategic capability.
- Open and re-open "red" communication lines with members, traditional allies, and new partners to rapidly meet and mitigate threats.
- Use the skills and best practices developed previously to identify and monitor motivations and communications of non-traditional actors. Develop a faster tempo of operations and couple that with additional time and precautions for the confirmation of threats, especially when the potential of WMD effects are present.
- Explore ways to disrupt adversaries' decision-making processes in the EDT environment. Understanding the adversary's OODA loop will give NATO multiple points to intersect and disrupt decisions making.
- Operate under the assumption that adversaries understand NATO's decision trees and are actively working to undermine them. As a result, consider what counter-measures or redundancies are required in critical infrastructure and systems.
- Develop systems and processes, so that NATO's humans-in-the-loop aren't disrupted by adversaries operating without such constraints





OUT-PARTNER THE ADVERSARY

How can NATO, its members, and affiliated organizations out-partner the adversary? How do they foster mutually beneficial, supportive, and habitual relationships with allied entities that can assist in such crucial areas as mitigation, deterrence, and recovery from threats? What exercises, organizations, and relationships are necessary to forge those links? -And how should they expand those links beyond traditional nation-states and their militaries? We address these questions in the recommendations provided below.

1. **COOPERATIVE WARGAMES.** Here we refer to simulations, exercises, and scenarios to model threat behavior along with the anticipatory and post-event actions NATO and its partners might take together to disrupt, mitigate, and recover from threats.

Wargaming and joint exercises have been essential tools for NATO cooperation and cohesion since the alliance's formation. In this spirit, NATO should not only update its wargaming and planning playbooks to account for the special characteristics of EDTs, but also as a means to engage with new partners at different scales (e.g., international, national, local), among different disciplines (e.g., technological and biogenetic), and within different sectors (e.g., governments, NGOs, private sector). To that end, our recommended actions for NATO are to:

- Conduct joint exercises involving rapid escalation and WMD use by nation-state actors; mass casualty EDT threats by non-nation-state actors; long-game attacks by insider threats, and related scenarios—including selective, non-NATO participants in the process. These exercises should aim to explore both successful mitigation efforts and attempts to recover from well-executed attacks.
- Develop international- and national-scale emergency plans with plug-in options for allied and partner governments as well as for private industry and NGOs, etc.
- Conduct cybersecurity exercises with industry partners to identify and mitigate vulnerabilities potentially exploited by adversaries.

2. **POLITICAL SOLIDARITY.** This means relationship-building, diplomatic programs, values declarations, and informal policies, especially aimed at non-NATO countries and international organizations for the development and mitigation of EDTs.

As a political counterpart to wargaming and military exercises, NATO should strategize how best to build support outside the alliance for the types of regulations and restrictions needed for monitoring, deterring, and interdicting EDTs (for more, see Out-Pace the Adversary above). Here we recommend efforts be targeted to:

- Encouraging and facilitating relationships between all nuclear powers, including traditional adversaries to mutually enhance NC3 systems against breaches by EDTs.
- Building of a coalition of global economic partners to support NATO's efforts to steer the development of dual-use EDTs.
- Looking for appropriate opportunities in Africa to increase cooperation, counter adversarial use of the continent as political proxies, and building local capacity to confront non-nation-state actors.

3. GOVERNMENT-MILITARY-CIVILIAN COOPERATION. With this, activities include coordination efforts between civilian governments, NGOs, and national militaries designed to successfully mitigate, deter, and/or recover from a threat.

Given the scope of both potential actors and potential targets for EDTs, it's necessary to cultivate a whole-of-alliance and whole-of-society response to mitigating these threats. This will require closer coordination between NATO members' militaries, governments, and civil society, with the goal of forging a social consensus around the risks of EDTs in conflict escalation. To this end, we recommend NATO:

- Encourage engagement across each member's military, civil, and security communities with a focus on educating civilian institutions about the threats and responses to EDTs.
- Partner across member governments and private industry to influence key international technology standards to guide the development of EDTs.
- Expand existing relationships to include non-military defense and security elements. Establish planning conferences to develop whole-society responses to non-military threats and create corresponding exercises to test and validate those plans.
- Determine new, non-traditional partners in future mitigation-and-recovery efforts, ranging from multinational conglomerates and supply chains (e.g., Amazon, Walmart) to civil society organizations. Identify what the Defense Industrial Base looks like in the future of EDTs. Determine how to positively influence global conglomerates to lead with a sense of global social responsibility in crisis.
- Research the social conditions and policies (e.g., poverty, inequality, racism, marginalization) that breed non-aligned cyber actors, which may intentionally or inadvertently interfere with national security capabilities. Share best practices among alliance members to resolve these conditions.
- Open doors to anyone with the skills and experience to serve the NATO defense community, even in cases where physical disability or neurodiversity preclude

conventional military service.

- Consider alternative criteria to meet NATO membership. In the era of EDTs, answer the question: what do defensive non-military contributions look like?
- Consider alternative criteria to meet NATO membership. In the era of EDTs, what do defensive non-military contributions look like?



OUT-LAST THE ADVERSARY

How does NATO, its members, and their societies out-last the adversary? How do they achieve and maintain a long-term perspective on potential threats and cultivate a culture of resiliency in response? We answer these two questions with the following recommended steps.

1. **EDUCATION.** Activities that fall within education include workforce education and training, vocational education, and retooling education pipelines to build the necessary skills for understanding, developing, and mitigating EDTs.

Many of the technologies under the heading of EDTs, including robotics, AI, and biogenetics are already at the center of conversations around the future of talent, jobs, and economic growth. Building an alliance capable of meeting the threats posed by EDTs will require cultivating a workforce and a talent pool equal to the challenge of developing and/or combatting them. Recommended activities for NATO include:

- Forging a consortium of global subject matter experts (SMEs) to address the implications of EDTs and their cultural impact.
- Revamping members' immigration policies to support, resettle, and re-train educated refugees.
- Broadening public awareness of disinformation, with continuously updated examples of its use by adversaries to sow mistrust.

2. **INVEST IN AND INCLUDE PEOPLE.** Here we refer to investigating and investing in human and social programs, including marginalized groups, subject matter expertise, and programs allowing for the redress of grievances.

Perhaps the best preventative measure against future EDT attacks by non-traditional actors and insider threats is to turn potential adversaries into allies before a potential attack occurs. NATO and alliance members should do this through investing in people, which not only means developing talent, but also resolving conflicts, reaching out to marginalized communities, and eliminating the conditions that foster radicalization. To accomplish this, we recommend NATO:

- Create an early-stage talent pipeline through partnerships with schools, private industry, non-NATO member states, and hacker communities.
- Practice the inclusion of marginalized and underserved communities, increasing communication and expanding efforts for conflict resolution.
- Invest in a fusion approach, convening diverse communities with global subject matter experts to discuss problems and strategize mitigation and recovery from an EDT or WMD attacks.

3. DEVELOP RESILIENCY. Here, we refer to programs and processes ensuring redundancy of essential services and infrastructure, and the development of a society-wide will to fight through difficult and uncertain circumstances.

When Russia invaded Ukraine in February 2022, many in the national security community predicted a swift outcome favoring the aggressor. However, the tenacity exhibited by Ukraine's civilian leadership, military, and society took many by surprise, including Russian leaders. What can NATO do to develop this type of resilience in the face of an adversary armed with EDTs and/or WMDs? How should members prepare, train, and rehearse for attacks on their armed forces, infrastructure, and shared identity? In order to plan for the unthinkable, we recommend NATO:

- Foster a cross-member and cross-sectoral approach to resilience, specifically focused on the aftermath of WMD attacks or long-game WMD effects. These strategic preparations and rehearsals should include both physical assets and systems as well as psychological support.
- Prepare for attacks and recovery through rehearsals with supply chains, medical responsiveness, backing up critical infrastructure, and delivering humanitarian aid.
- Strengthen defenses against pre- and post-attack misinformation, designed to sow mistrust and delay recovery efforts in the wake of attacks.
- Periodically catalog supply chains for components of both EDTs and critical infrastructure. Determine if new supply options and commodity resources are needed, and support alliance members' investments in these options.
- Prepare for attacks and recovery through rehearsals with supply chains, medical responsiveness, preparing back up critical infrastructure, and delivering humanitarian aid.
- Strengthen defenses against pre- and post-attack misinformation, designed to sow mistrust and delay recovery efforts in the wake of attacks.
- Periodically catalog supply chains for components of both EDTs and critical infrastructure. Determine if new supply options and commodity resources are needed, and support alliance members' investments in these options.



IMPLICATIONS

OVERVIEW

Using the Threatcasting Methodology, we envision a range of possible and potential WMD and EDT threat futures in the 2040 timeframe. The future models assume a high level of EDT development between now and 2040. Our goal in providing this report is to explore the possible and potential attack surfaces and vulnerabilities that will be opened for EDT development and their use in the future as well as how they might be paired with WMDs.

In this section, we outline seven implications for the current state and strategic path for NATO. We also define opportunities and critical enablers for NATO and members to prepare for these threats. Finally, where appropriate, we explore the potential impact on North Atlantic Treaty Articles 3, 4, and 5.

Functionally, each of the following implications can feed into NATO's existing and planned investments and activities. For each threat future, the use of EDTs and WMDs will necessitate an expansion of the definition and implementation for the concept of integrated deterrence. Additionally, many of the suggested activities can serve as the focus areas of research, discussion, and challenges for the forthcoming DIANA and triple-helix centers or programs.



IMPLICATION #1: NATO SHOULD WIDEN THE NUCLEAR FIREBREAK TO MINIMIZE CONFLICT ESCALATION.

DEFINITION:

In fire sciences, a firebreak is a purposefully carved zone of earth, bare of flammable vegetation that contains the effects of a wildfire. In rugged terrain and uncertain weather conditions, these firebreaks must be dug where firefighters can most effectively reach them and not necessarily at the global optimal position. Sometimes, the firebreaks help fire fighters prioritize saving some parts of the landscape over others. Attacks on critical infrastructure may be a prelude for escalating conflict into the lethal and nuclear zone of conflict. So how does NATO widen the nuclear firebreak, and where does the Alliance take risks? We address these questions below.

Current State and Strategic Path:

To understand how NATO might slow down conflict escalation accelerated by EDTs, effectively widening the nuclear “firebreak”, it is helpful to understand and dissect how EDTs might bring about an increased

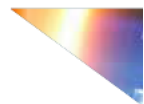
nuclear risk.

A study by Marina Favaro at King’s College London used Machine Learning (ML) to group expert assessment of emerging technologies into four clusters, especially as they relate to nuclear risks.⁴⁸ These EDT effects include distortion, compression, thwarting, and illuminating adversary actions and intentions. Distortion, compression, and illumination are concepts clearly identified in our study. Favaro only considered directed energy weapons as a thwarting technology, which is an EDT not within the scope of our study.

Although Favaro describes the effects of emerging technologies to nuclear risk at a fairly high level of abstraction, the framework of distortion, compression, thwarting, and illumination applies to understanding the effect of EDTs on other WMDs and to traditional NATO military operations. In fact, Favaro’s framework provides a clever vocabulary that can be further explored as an ontology of describing a wide variety of the disruptive effects of EDTs. Some examples follow:

1. The first cluster, **Distortion**, is when adversaries interrupt data flows and position the information landscape to their advantage. Examples of distortion include propaganda, mis/disinformation, and information warfare. Their purpose is to sow uncertainty and “undermine public trust

⁴⁸ Favaro, *Weapons of Mass Distortion*.



in social media and damage online civic culture” (p. 12). WMDs layer particularly well with technologies of deception. They create the perfect false flags because the idea of their use is unbelievable.

The most troublesome technology that Favaro’s experts agreed distorted information was the use of “deep fakes”. The power of deep fakes is amplified by advanced computing and social media content delivery algorithms.

Deep fake technologies are built on the backs of AI facial recognition, voice recognition (e.g., Siri and Alexa, etc.), and speedier hardware and software systems that create increasingly realistic adaptations of source material. Additionally, sophisticated deep fakes may even deceive the ability of national intelligence to make error-free conclusions. This means decision-makers may have to rely on compromised intelligence before deciding on a first-strike option.

Much of the technological amplification associated with distortion originates in the private sector. Therefore, addressing distortion effects must be done by engaging the private sector rather than leaving NATO as a military and political organization to solve it on their own.

2. The second cluster, **Compression**, happens when the speed of conflict reduces the time available to decision

makers. The technologies that compress decision making include AI-powered cyber operations, hypersonic missiles, and swarm robotics. Experts in the King’s College report assess these effects to have a high impact, but low feasibility of implementation.

The report also suggests that decision makers should be wary of over-hyping some of these technologies. It calls out that hypersonics are “merely an old technology with a massive price tag and few meaningful advantages over existing ballistic missiles”.⁴⁹ On the other hand, hypersonic missiles “could accelerate an ongoing crisis by compressing decision-making time or by enabling a disarming first strike”; therefore, making it the most impactful EDT related to nuclear stability and decision making. There is no clear consensus on an objective impact of hypersonics, other than the fact that they potentially compress decision-making timelines to unrealistic extremes.

3. The third cluster, **Illumination**, refers to how intelligence agencies illuminate adversary actions and intentions. As the amount of data increases what ISR sensors collect, intelligence agencies must turn to automated tools and AI to sort, categorize, and make sense of massive amounts of data. “Although the incorporation of ML and autonomous systems can lessen the data searching, processing, and analysis burden for human command, the inclusion

of technical elements contribute to system complexity and so create a new source for errors, biases or vulnerabilities hidden from operators.”⁵⁰ To “Out-Think” adversaries, NATO must simultaneously incorporate appropriate AI, ML, and autonomous processes, while simultaneously studying for new sources of errors and bias, including whether sensors are being spoofed or deceived. OpenAI recognizes adversarial AI research as a potential field to study how AI can be spoofed or deceived.⁵¹

The key to minimizing the impact of EDTs on the lethality of WMDs is to counteract the forces of distortion and compression, while encouraging illumination. NATO must lobby for the recommendations in the “Outs” section be placed into members’ budget priorities. This must be done in such a way that one country does not “shoulder the burden” of responding to a single technology alone. Deconflicting research, development, and communal response requires a focus on the distribution of tasks and responsibilities.

While it is true that many of the actions in the “Outs” should be led by military forces and organizations, much of the EDT ecosystem spans the public-private divide. This means that member nations must invest in EDT strategies and GDP expenditures that consider cooperation with private research, development, and dual-use

technologies.

NATO’s Defence Innovation Accelerator for the North Atlantic (DIANA) and its supporting research centers could be NATO’s think-tank for EDT threat analysis, in addition to its research, development, and commercialization arm. Cooperative partnerships from academia, government, and private industry sectors, the so-called triple-helix, also plays a role in assisting NATO to develop processes to measure EDT threat emergence, metrics of security risk, and the ability to communicate EDT threats to deterrence strategy.

Opportunities and Critical Enablers:

NATO can be a leader of defining human, technical, and hybrid human-AI teamed firebreaks in NC3 systems. It can also be a critical enabler to ensure safeguards, such as human-in-the-loop procedures, deliberate fact checking, and frequent rehearsals remain in place.

Implications to the Treaty:

NATO must consider how the development of EDTs in the private sector creates situations that reduce the nuclear “fire-break”. Within Article 3, members must account for the resiliency necessary to resist pre-cursors to an armed attack. Specifically, with the development of mis/disinformation technologies, processes,

49 Cameron and Wright, *Don't Believe the Hype About Hypersonic Missiles*, 15.

50 Favaro, *Weapons of Mass Distortion*, p21.

51 OpenAI, *Attacking Machine Learning with Adversarial Examples*, 17.

and deliberate operations to distort truth and compress decision-making timelines. This may require more frequent deliberation with the North Atlantic Council, heads of state, and the European Council about the increased use of distortion and compression technologies..

IMPLICATION #2: NATO SHOULD RAISE THE BAR FOR THE INTENT TO USE WMDs.

DEFINITION:

In the future, EDTs can create a condition where the intent to use WMDs is increased. Lowering the “taboo” or bar to using a nuclear device is the greatest threat. Conversely, raising the bar helps slow the spiral of escalation to WMD use, most importantly in the use of non-strategic, tactical nuclear weapons during military conflict situations. These conflict situations might include so-called “grey space” operations in the competition phase before force-on-force conflict occurs.

While most countries steadfastly maintain that their WMD arsenals are defensive or deterrent, the fact remains that WMDs are most effective as first-use weapons. The first shocking attack generates a surprise element. After that, however, the enemy will almost always recover and adapt. Because of this as well as the fact that they have such a powerful psychological effect, WMDs tend to be less effective after the first surprise attack



Current State and Strategic Path:

The use of EDTs on the “attack plain” creates a sense of being “backed into a corner” for the adversary to the extent that they feel their only recourse to restoring a power balance with NATO is a nuclear response. They are likely to strike hard with the most powerful weapons at their disposal. The psychological pressure of being backed into a corner by EDT dominance may also apply to nuclear powers that are not traditional nuclear weapon states (NWS) as defined by the Treaty on the non-Proliferation of Nuclear Weapons (i.e.; United States, Russia, the United Kingdom, France, and China).⁵² These “non-NWS” (e.g., India, Pakistan, North Korea, Israel, etc.) could feel in the face of EDT dominance, that all other tools of national power (e.g., diplomatic, information, and economic) are not going to give them the changes they want to see in the world. Likewise, they may think they are out-matched or “out-teched” in the ability to employ EDTs to accomplish their strategic plans. In other words, an actor may feel the push to use WMDs because of the perceived gap in their ability to employ EDTs.

As a recent historical example, one of the great threats of the Iraq War was the worry that U.S. and NATO’s use of force was so

overwhelming to Shia militia groups that the latter would feel they had no recourse, but to obtain nuclear material from Iran and conduct a high-profile attack against allied forces.

Additionally, the threat of EDTs could find an adversary with their “back against the wall”, employing a combination of EDTs in concert with non-nuclear WMDs to deliver attacks on NATO. It is trivial to imagine Syria lashing out with whatever combination of EDTs and WMDs they have access to. Case in point, combatants in Syria have attached hand grenades, mortars, and other explosive devices on disposable drones and flown them into Russian and American bases.⁵³ It is not difficult to imagine making this tactic more lethal by adding chemical or biological agents to the drones instead of grenades. Ensuring the bar remains high is necessary in this type of situation.

These two conditions largely apply to “non-NWS” nuclear powers, such as Iran, North Korea, Israel, Pakistan, India, and non-nation states. In the language of risk management, a threat must have both capability and intent for the risk to materialize. Raising the bar is the concept of inhibiting the capability of an actor to gain access to WMDs as well as impacting the intent of a nation-state actor to loosen requirements on the “taboo” of using nukes.

⁵² United Nations Office for Disarmament Affairs, *Treaty on the Non-Proliferation of Nuclear Weapons* (NPT)

⁵³ Woody, *Drones Are Being Used to Drop Bombs on US Troops in Syria*

Non-nation state actors, especially private corporations, control a tremendous amount of the EDT ecosystem. This is an important indicator of when "non-NWS" nuclear powers begin to seek out private corporations to buy, build, and/or develop EDTs. It is important to understand where the "bar" is at any given point by watching the development path of private industry and what the global adoptions of EDTs by militaries look like. There is a tipping point where EDT superiority creates a window of opportunity for an adversary to act.

Opportunities and Critical Enablers:

From a Treaty point of view, the emergence of EDTs and their influence on an adversary's intent to use WMDs, is a diplomatic and cultural problem rather than a non-proliferation or military problem. Prohibitions, constraints, and norms on the use and development of many WMDs have been in place since at least the Lieber Instructions of 1863⁵⁴ and the Hague Regulations of 1899.⁵⁵

NATO and the major nuclear powers have worked tirelessly to keep nuclear precursor knowledge and materials out of the hands of non-nation states and "non-NWS" nuclear powers. At the same time, NATO needs to lead a strategic discussion on the prohibitions of EDTs that lowers the bar for using nuclear weapons.

On the one hand, the prohibition on the

use of WMDs and nuclear, biological, and chemical materials are controlled by international agencies and treaties. NATO and its member nations are keenly tied into these organizations, treaties, and laws. On the other hand, there are few controls on the development and use of most EDTs in our study. The development of lethal autonomous weapons systems (LAWS) is the most contested.⁵⁶ Hypersonics, AI, and designer drugs are EDTs from our data models that have been considered as "arms-race" topics.

A course of action for NATO to consider is to participate in ongoing debates on some of these EDTs. NATO should be prepared to accommodate potential solutions, including limitations, moratoria, prohibitions, and acceptable norms on the use and further development of hypersonics, AI, LAWS, and designer drugs. As an active participant in recent conflicts in Iraq, Syria, and Afghanistan, NATO has witnessed firsthand how the future of EDT-enabled conflict is emerging. NATO could become a trusted voice in leading and participating in these types of discussions.

Implications to the Treaty:

Article 3 of the Treaty requires member states to develop an individual ability to resist armed attack. In the future, this might be used in preparation for the “non-use” of certain levels of EDTs. This translates into the development of doctrines and norms for acceptable and appropriate use of EDTs. Conflict and competition could be part of the development of a culture resisting armed attack through preparedness.

Article 4 consultations would be a logical and necessary next step if, in the future, an EDT or combination of EDTs, meets the threshold of an attack being imminent or inevitable. Indicators of an imminent threshold situation could start with the use of non-nuclear WMDs, such as arming make-shift drones with chemical or biological agents and continuing the escalation until a desperate nuclear option is the only choice left. This would be preceded by rapid advances in EDT acquisition and employment by NATO nations and slow advances by “non-NWS” states.

IMPLICATION #3: EXPAND NATO’S UNDERSTANDING OF INSIDER THREATS AND MOTIVATIONS.

DEFINITION:

There are channels that connect insiders to outside narratives, identities, and forces that cause them to act against NATO. The increased speed, scope, scale, and impact of an attack from a single person are amplified with the use of single or combined EDTs. Insider threats pose a threat because of their placement and access within organizations. In the future, it will be possible for an individual to have an outsized effect on NATO members using EDTs. Insider threats are particularly dangerous when this access and outsized EDT effect are combined.

Typical insider threats with financial, ideological, and/or political motives will remain a persistent and constant threat. However, in the future, the “unknowing” insider threat could become even more dangerous. An unknowing insider threat would be a person inside an organization who

54 International Committee of the Red Cross, *Treaties, States Parties, and Commentaries - Lieber Code*.

55 International Committee of the Red Cross, *Treaties, States Parties, and Commentaries - Hague Declaration (IV/2) Concerning Asphyxiating Gases*.

56 Sayler, *International Discussions Concerning Lethal Autonomous Weapon Systems*.

has been compromised without their knowledge, typically via their devices or computer accounts. There is a specific subset of EDTs that are more likely to be used to perpetrate and amplify an insider-based attack. These include AI, IIoT, and autonomous systems, such as drones, self-driving vehicles, automated decision making, etc. This person would then be operating inside the organization, giving an adversary access without the person's knowledge.

What is particularly troubling about this specific kind of insider threat is that guarding against it will be difficult. Traditional insider threats reveal specific clues or activities, which can indicate that the threat exists. However, in the case of the unknowing insider threat, there are no traditional clues. In fact, there may be no clues at all, only the presence of one or more EDTs.

Current State and Strategic Path:

Insider threats are a known vulnerability within all organizations. The unknowing insider threat is currently a possibility, and the introduction of EDTs into an organization and the insider threats personal device(s) increases the likelihood and impact of the threat. Research by NATO's Cooperative Cyber Defence

Centre of Excellence (CCDCoE) in Tallinn, Estonia, recognized the possibility of the unintentional insider, largely as a vector for providing access for any number of cyber threats or because of accidental disclosure of proprietary information. Unfortunately, the CCDCoE provides no additional information about the uniqueness of an unintentional insider as compared to a purposeful insider, or recommendations about how to detect or thwart them.

The strategic path to this threat requires a combination of cultural and psychological factors that will remain largely the same in the future. The key behaviors to watch out for are the adoption and use of EDTs in the organization and its staff's personal use.

Culture, race, and religion are also critical factors in the use of WMDs. It is much easier to use WMDs on people you consider as lesser beings. Even when technologies of mass destruction were banned in European warfare, many, if not most, technologies were acceptable when used to exterminate indigenous people in colonial contexts. Culture, race, religion, and other socioeconomic factors will remain prevalent, in the future, about whether or not to use WMDs

Opportunities and Critical Enablers:

A critical enabler for NATO is to lead an effort to develop a clear strategy for monitoring and training around insider

threats for all members. What's also needed are metrics for measuring the impact of the insider threats and their motivations.

NATO should also explore the new category of the unknowing insider threat, exploring speed, scope, and scale of how EDTs affect a person who becomes a carrier of the threat. This would also include training to safeguard people within organizations against manipulation and systems that can monitor for this type of activity.

Implications to the Treaty:

It will be important to have a well-articulated strategy for monitoring insider threats, training for individuals within organizations, and creating an environment of resilience. These could be seen as a part of Article 3's preparedness.

If the presence or activity of a singular insider threat has been detected, it will likely be the purview of that Alliance member to contain and mitigate that threat. If a systemic insider threat materializes through the combination of multiple EDTs or if metrics that measure the impact of the insider threat reach a certain threshold, NATO members could trigger Article 4 for a collective response to the threat, technology, and/or condition underlying it.

IMPLICATION #4: NATO SHOULD ADDRESS PLAUSIBLE SCENARIOS OF EDTS INTERACTING WITH EACH OTHER AND WITH WMDS.

DEFINITION:

Beyond attacks on critical infrastructure, the combination of multiple EDTs will also bring about WMD effects. It is necessary for NATO to understand the full extent of multiple EDTs interacting with each other to provide sufficient detection mechanisms, preparedness, resiliency, and changes to collective defense measures. This understanding also requires NATO to consider the dual-use effects of EDTs for their intended scientific, social, and business applications, while simultaneously being used for conflict.

Current state and Strategic Path:

Currently, most EDTs are being developed by private industry, especially in western democracies. Apart from China and to a lesser extent Russia, who both have maintained significant state control over research and development, advances in

EDTs will happen outside of the control of NATO and its members.

NATO does not have a mechanism for tracking the development of EDTs so that members can know when an EDT has reached a point where it can be used as a weapon. What is essential to identify is, how NATO knows when an EDT has become too dangerous. Addressing this after it exists is too late.

As NATO considers combinations of EDTs in scenario exercises, assume multiple WMDs are involved. Layering and combining EDTs massively amplifies their lethality. This is true of cyber and just about any of the others. Because so much about using WMDs is about mind games, deliberate confusion, and outflanking enemy expectations, WMDs are often used in concert to amplify or ensure their effect.

Case in point, agriculture is an extremely effective target that tends to get overlooked because it's not alluring nor flashy. A biological weapon attack on staple crops, however, could cause epic damage to an economy, and cause famine as well as domestic chaos. This is a real threat, and a number of world powers have been victims of technologies designed to attack populations indirectly through their food sources, including ransomware,⁵⁸ IIoT hacking, and purposeful contamination with E. coli and Salmonella.⁵⁹

NATO and other organizations, such as the United Nations are exploring restrictions on the development and use of some EDTs, including lethal autonomous devices, and synthetic biology, etc. As expressed in implication #2, NATO does not yet have collective guidance on the full line up of EDTs explored in this report, or which EDTs require limits and restrictions.

Opportunities and Critical Enablers:

As a critical enabler, NATO can create a better understanding of the impact EDTs have on warfare through deliberate research, wargames and exercises, and consultation with the private sector organizations that are developing them. As explored earlier in the report, NATO can begin monitoring the development of the full spectrum of EDTs in this report and delegate research to all of its members and industrial counterparts.

Another critical enabler would be to explore the expansion of limits and restrictions on the development and use of all EDTs beyond the current activities, especially as it relates to their dual-use nature. Organizations such as NATO's Advisory Group on Emerging and Disruptive Technologies can lead responses to technology innovation that is driven largely by the private sector. In that vein, NATO should "Set out objectives for harnessing dual-use, multi-use technology developments – capitalising on already existing technology from other domains

and driving the development of multi-use outputs.”⁶⁰

Finally, NATO should develop critical enabler processes to monitor the use of single and combined EDTs, setting metrics for the measurement of when that EDT or combination of EDTs has the possibility of producing a WMD effect. NATO has recently revealed plans to develop a formal program that develops emerging technologies in a cooperative manner. Conceptually approved in NATO’s June 2021 Brussels Summit, The DIANA was approved by allied foreign ministers in 2022. DIANA “is designed to harness new academic, commercial, and entrepreneurial start-up technology, test and develop it as potential defence capability, and connect it more quickly to military end-user operational requirements.”⁶¹ DIANA’s concept of nearly 50 test centers and accelerator programs is an ideal place for NATO to iterate and consider the implications of EDTs as they affect strategic and operational requirements.

Implications to the Treaty:

As a part of the preparedness intent of Article 3, members should develop tools and processes to track, monitor, and communicate the development of EDTs to the Alliance.

Using an agreed upon future metric for the use of a single or combined EDT, members can evoke Article 4 when a threshold of security threat is reached.

IMPLICATION #5: NATO SHOULD MEASURE AND STABILIZE COMPLEX SYSTEMS.

DEFINITION:

For EDTs or a combination of EDTs to have a WMD effect, they primarily need to have the capacity to attack complex systems and/or critical infrastructure. The destabilization of one or more aspects of critical infrastructure is what can produce the destabilizing and lethal WMD effect(s) without the actual use of a WMD. Therefore, to monitor, disrupt, or mitigate this kind of threat, it is important to have a functional definition of what these complex systems or critical infrastructure might be.

The United States Cybersecurity and Infrastructure Security Agency (CISA) defines critical infrastructure in the following way: “There are 16 critical infrastructure sectors whose assets,

58 McCrimmon, Ryan, and Matishak, *Cyberattack on Food Supply Followed Years of Warnings*. See also: Fagan, *Critical Vulnerabilities in the U.S. Food Sector and the Next Crippling Attack*.

59 Sobel, Jeremy, Khan, and Swerdlow, *Threat of a Biological Terrorist Attack on the US Food Supply: The CDC Perspective*.

60 NATO Advisory Group on Emerging and Disruptive Technologies, *Annual Report 2020*.

61 Willett, *NATO Details DIANA Technology Programme*.

systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”⁶²

The sixteen U.S. critical infrastructure sectors are:

- Chemical,
- Commercial Facilities,
- Communications,
- Critical Manufacturing,
- Dams,
- Defense Industrial Base,
- Emergency Services,
- Energy,
- Financial Services,
- Food and Agriculture,
- Government Facilities,
- Healthcare and Public Health,
- Information Technology,
- Nuclear Reactors/Materials/Waste,
- Transportation, and
- Water/Wastewater Systems.

The European Union has a similar, but slightly different definition. European Critical Infrastructure (ECI) means “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal

functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.”⁶³ A European think tank has added, “Damage or destruction of critical infrastructures by natural disasters, terrorism and criminal activity may have negative consequences for the security of the EU and the well-being of its citizens. Thus, it is very crucial to protect the ECIs since they play vital role for the functioning of a society and economy.”⁶⁴

The eleven ECI sectors are:

- Energy,
- Information and Communication Technologies (ICT),
- Water,
- Food,
- Health,
- Financial,
- Public & Legal Order and Safety,
- Transport,
- Chemical and Nuclear Industry, and
- Space and Research.

Current state and Strategic Path:

Across the NATO members, there is no universally agreed upon definition of critical infrastructure, although many European nations have adopted the ECI sectors. For this report, we are using CISA's framing of the problem and CISA's list of critical infrastructure.

Since 1949, as mentioned earlier, the Allies have invoked Article 5 once, within 24 hours of the 9/11 terrorist attacks in the United States. The Allies have also put collective defense measures in place five times since 1949. These include three instances of a request by Turkey: in 1991 with Patriot missile deployment during the Gulf War; in 2003 for Operation Display Deterrence during the Iraq crisis; and in 2012 with Patriot missiles in support of the situation in Syria. Additional collective measures included: tripling the size of the NATO response force; improving Joint Intelligence, Surveillance, and Reconnaissance; and air policing over the Baltic and Black Sea areas after Russia illegally annexed Crimea in 2014. In February 2022, NATO mobilized additional forces and put the NATO Response Force into a deterrence posture following Russia's invasion of Ukraine.⁶⁶

Although NATO does not have an agreed upon definition of critical infrastructure,⁶⁷ it has reinvigorated the efforts of "civil preparedness" that dropped in priority following the end of the Cold War. Resilience, as a national and collective value, is closely tied to the protection of critical infrastructure and to the tenets of Article 3. The seven baseline requirements for civil preparedness are outlined in the 2016 Warsaw Summit and include collective responses to responding to terrorist threats or nation states. These baseline requirements are:

- 1) Assured continuity of government and critical government services;
- 2) Resilient energy supplies;
- 3) Ability to deal effectively with uncontrolled movement of people;
- 4) Resilient food and water resources;
- 5) Ability to deal with mass casualties;
- 6) Resilient civil communications systems; and
- 7) Resilient civil transportation systems.⁶⁸

Opportunities and Critical Enablers:

A critical enabler would be for NATO to establish a working definition of complex systems and critical infrastructure for its members. This includes setting standards

62 Cybersecurity & Infrastructure Security Agency, *Critical Infrastructure Sectors*.

63 The Council of the European Union, *The Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*, 75–82.

64 SPEAR Project, *A Review of Critical Infrastructure Domains in Europe*.

65 North Atlantic Treaty Organization (NATO), *Collective Defense - Article 5*.

66 Ibid.

67 Lucia, *Critical Infrastructure Protection*.

68 Roepke, Wolf-Diether, and Thankey, *Resilience: The First Line of Defence*.

for measuring levels of contributions to NATO-wide civil preparedness and measurements to identify and describe emerging threats due to EDTs. NATO clearly understands the involvement that the European Union has in administering the critical infrastructure architectures and the relationship with the commercial sector. At the same time, what's lacking are mechanisms and procedures on testing how the civil sector and NATO should cooperate during a real-event.

NATO members can engage the political elements of their countries to ensure that CIP processes expand beyond "prevention, preparedness and response to terrorist attacks" as outlined in a 2006 communication from the Commission of the European Communities.⁶⁹ This approach expanded the work on critical infrastructure protection to thinking beyond terrorism and into an "all-hazards approach". The European Union recognizes that, "Threats cannot be seen in a purely national context. The interconnected and interdependent nature of today's economy and society means that even a disruption outside of the EU's borders may have a serious impact on the Community and its Member States."⁷⁰

Implications to the Treaty:

There are many differences between definitions of armed attack, and it's probably one of the most contentious stumbling blocks to a consensus on including destabilizing attacks short of an

"armed attack" into the Articles 4 and 5 counter-escalation cycle. The development of threats to critical infrastructure by EDTs is arguably the next iteration in the development of civil preparedness mechanisms for member nations.

The ability for NATO members to measure levels of destabilization on critical infrastructure via an EDT attack is essential to measuring the effectiveness of NATO and civil preparedness efforts. When a perceptible level of destabilization is detected that threatens security, as

DEFINITION:

There are a number of factors that inhibit adversaries from successfully playing a long game. Some of these include the compression of decision-making time, lowering the bar for the use of WMDs, growing concern over insider threats, and the societal dependence on critical infrastructure. The use of single or multiple EDTs will allow adversaries to initiate long-term strategies, using the technologies over an extended period of time to achieve WMD effects. Truly understanding this requires a mindset shift. The EDTs will enable a long-game attack that we will not see as an "attack". Without ignoring the need

to occasionally interrupt or change both the weapon and EDT systems in the short term, NATO must see the development of EDTs in this threat space over a long period of time. An example of a long-game strategy that purposefully pushes against the red line of aggression is Russia's involvement in Crimea and Ukraine. Russia's strategy of making small territorial and political incursions into Ukraine (also called "salami tactics," reminiscent of making very thin slices of the meat that slowly stack up) induces a *fait accompli*, to which the UN and NATO have no option but to accept Russia's newly gained territory, or risk escalation to war. This challenges the world's resolve in responding to Russia's advances in Ukraine as Russia takes more liberties the longer the UN or NATO does not respond.

measured by some standard of pre-established metrics, it could rightfully trigger the consultation requirement in Article 4.

Validation of perceptible destabilization, such as with an armed attack with EDTs or combinations of them, could trigger collective defense in Article 5.

IMPLICATION #6: NATO SHOULD DEVELOP A SOLUTIONS MINDSET FOR LONG-TERM POTENTIAL ATTACKS.

Current state and Strategic Path:

With the current definition of WMDs and WMD effects, there is no exploration or specific framework for how a long-game attack might present itself. Because these attacks are designed to remain "under the radar", they will present themselves as criminal attacks, glitches in the system, or may remain hidden completely until their effects cannot be reversed.

The further development of EDTs by private industry will increase the hidden nature of their development. Additionally, because these EDTs will come out of industry, any attack or early indicator of an attack will present itself as a private sector crime or anomaly. NATO members may not even know that they are under attack from an adversary.

Opportunities and Critical Enablers:

Another critical enabler would be for NATO to work with members to develop processes, procedures, tools, and metrics for monitoring long-term EDT effects. This might be accomplished by methodically simulating a number of

plausible combinations of EDTs, WMDs, and conventional attacks. This would help members discover common, observable indicators that could be developed into formal intelligence requirements for the Alliance. A new strategic planning group would also need to be empowered to affect long-term strategies, contributions to collective defense, and security guidelines.

There is a risk, when sensing for a long-game attack, that a NATO member could be seen as monitoring noise or even being overzealous. For example, in April 2022, social media users noticed a seemingly suspicious number of fires at food processing plants around the United States, leading media personalities, such as Turning Point USA founder, Charlie Kirk, to declare on Twitter, “Our food supply is under attack – the question is, by who?”⁷¹ In fact, the fires were determined to be accidental and not statistically anomalous.⁷² The lesson here is that facts did not deter social media users from continuing to push for an investigation.

NATO has an opportunity to work with members and their critical infrastructure and industry partners to begin sensing and measuring potential impacts in “grey space”. Along with this sensing, a metric can be established to indicate when the activity being observed has moved from private sector crimes or anomalies to an EDT attack. Typically, this type of attack can

be measured by its destabilizing effect on critical infrastructure.

Implications to the Treaty:

DEFINITION:

The access to and increased effectiveness of future EDTs will allow non-traditional adversaries to attack NATO members. These adversaries will include non-nation state groups as well as corporations.

Similar to section 5 above, as a part of the preparedness intent of Article 3, members could develop tools and processes to track, monitor, and communicate the development of EDTs to the Alliance. Using an agreed upon metric for the use of a single or combined EDT, members would be able to evoke Article 4 when a threshold of security threat is reached.

IMPLICATION #7: INTERACTION WITH NON-NATION STATES AND CORPORATIONS

Current state and Strategic Path:

Currently, NATO does not have a way of guarding against or taking action against non-nation state or corporate actors. This is particularly troubling because of Europe’s history with non-nation states and

colonialism.

The current international framework of a state-based system is based on a system that was originally European in design. Non-Europeans have learned to “shoehorn” themselves into this framework.

The state is a modern political construction that, in large part, grew out of the experience of European conflicts like the Thirty Years War. The state is a system of order that, in the words of political theorist Max Weber, “claims the monopoly of the legitimate use of physical force within a given territory.”⁷³ To be a state in our contemporary consideration, a system of human organization must have a dominant claim to three things: (1) an organized administrative system that (2) holds exclusive control of the use of force (3) in a defined territory or space. The concept of the state, however, has evolved significantly over the course of the past centuries. Current definitions of State and Nation are provided below.

State: “the body politic as organized for supreme civil rule and government; the political organization which is the basis

of civil government (either generally and abstractly, or in a particular country); hence the supreme civil power and government vested in a country or nation... A body of people occupying a defined territory and organized under a sovereign government.”⁷⁴

Nation: “an extensive aggregate of persons, so closely associated with each other by common descent, language, or history, as to form a distinct race or people, usually organized as a separate political state and occupying a definite territory.”⁷⁵

The combination of the two into the term nation-state implies a system of order wherein the nation and the state are at least roughly congruent. In Post-Westphalia, we see a clearer overlap of these two ideas, which develop in tandem though not always in the same direction. A nation-state, then, is a system of order that expresses power over both borders and peoples.

It follows then, that a nation-state would have control over all of the following:

- Territory and space,
- Bureaucracy and administration,
- Use of force and sovereignty, and

71 Kirk, Charlie (@charliekirk11). 2022. “Food processing plants don’t just ‘accidentally’ burn down at this rate and they certainly don’t ‘coincidentally’ become landing pads for plane crashes at the rate they are...Our food supply is under attack in America. The question is—by who?.” Twitter, April 29, 2022, 6:43PM.
https://twitter.com/charliekirk11/status/1520171930325643266?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1520171930325643266%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Farticle%2Ffactcheck-processing-fire-idUSL2N2WW2CY.

72 Reuters Fact Check, *Fact Check-Food processing plant fires in 2022 are not part of a conspiracy to trigger U.S. food shortages*.

73 Weber, *Politics as a Vocation*, as quoted in state monopoly on violence.

74 *Oxford English Dictionary*, second edition, senses 29 and 30.

75 *Oxford English Dictionary*, second edition.

- A people or peoples (i.e., the dictionary idea of a "common descent, language, or history").

A nation-state's legitimacy is defined by its control over those four areas, like the four legs of a chair. Some challenges have the effect of eating away at legitimacy like termites in the wood until the chair collapses. Other challenges are more comparable to attacking a chair's legs with an ax. Continuing with this metaphor, with careful balance, the chair can probably hold up on three legs for a time, but as heavy ideological weight puts continued stress on the chair, it will eventually collapse.

A comparable analogy is illustrated with 20th-century anti-colonialism, where challenging questions emerged, such as "who gets to define who 'the people are'?" or "when is the use of force against the state justified?" It seems that often such challenges happen where the overlap between nation and state is critically limited.

In addition, the digital world complicates the idea of territory and space. Our current ideas of territory and space are changing as we absorb the implications of cyberspace- in terms of how we conceive of and use physical as well as virtual artifacts to define them. In the modern era, from the 15th-20th centuries, the struggle over control of land has been a defining characteristic. In the new era of the 21st century with cyber,

different struggles may define the position of physical territory.

Both the rise and fall of colonialism are central to our understanding of the modern nation-state. Things such as the concept of nations become defined on frontiers. These are the places where boundaries need to be defined and where people have the capacity to work through the process together (which has historically been done in a violent manner).

The modern global corporation was born in this context of the "frontier". Corporations have typically functioned in the hybrid space between economics and politics, acting at times to advance capitalist goals and at other times to advance political or social goals. The global corporation is even more capable of being larger than a commercial organization with a simple capitalist bottom line. In many cases, global corporations exercise state powers more often than most people would think possible.

It is important that NATO countries avoid getting too focused on the state- and non-state actors dichotomy. Their nature falls within a continuum, and they overlap. Instead, we recommend that NATO looks for motives and circumstances before categorizing actors. The thought here is to observe patterns before getting attached to a specific narrative about an actor.

Opportunities and Critical Enablers:

The emergence of EDTs will allow non-nation state actors and corporations to influence the global security stage. The reality of this future necessitates that NATO becomes a critical enabler in this area. NATO will need to expand its definition of possible and potential adversaries to include these non-traditional actors.

To do this, NATO should convene a working group to define these actors, their potential effect, and how to monitor and measure their rise to power. Working with NATO members, sharing information about the emergence of these actors and their early activities will be essential to take appropriate action at the appropriate time.

This could potentially be a “sacred cow” within the NATO construct, which allows them to start thinking now about how to interact with global, multi-national corporations, which take on more of what has been considered traditional nation-state activities and responsibilities. Doing so will yield positive results in the future.

Implications to the Treaty:

The definition, monitoring, and information sharing of these groups' activities should become part of Article 3's preparedness. The emergence and clear presentation of activities could be a trigger for Article 4.

STRATEGIC PATHS OF THREAT ACTORS

Each threat actor type explored in the

workshop and outlined in this report have different motivations. Each of these threat actors relate differently to the findings. Each one also has different capabilities and could exploit NATO and members' weaknesses in different ways. Furthermore, the actors could work together knowingly or unknowingly to bring about one of the six threats in the findings. These capabilities and interactions are outlined below.

One of the threat actors applies to all six findings. It is the Conditional State. The conditional state refers to the environment created by the development and emergence of EDTs. The increasing adoption and use of one or all of the EDTs together increases the likelihood that any one of the six findings will happen. Like the soil from which seeds grow, the conditional state is the environment from which these potential threats will spring. Understanding this environment and tracking its progress will be essential for the preparation against future threats

Single Actor without Support:

A single actor with no support from nation states or broader groups will have a limited potential for impact compared to the other two threat actors. However, the speed, scope, scale, and impact of EDTs, alone or combined, will make the single actor a significant threat.

The greatest probability of impact for this threat actor will be the New Insider Threats

(discussed in Finding #3) and The Long Game (addressed in Finding #6). EDTs will enable the single actor to act as an insider threat for financial or ideological gain. Here, the threat actor exploits the inherent trust of the organization's insider through which they work or operate. This kind of threat is not new, and it is much like a traditional insider threat. However, it is the outside impact of the EDTs that can make this threat significant.

Like the Insider Threat, the Long Game will allow a single threat actor to exploit a small opening or weakness to attack NATO and member EDT systems with an attack that will evolve over time. This longer timeframe allows the initial contact or scope of the attack to be small. It is with time that it will become significant.

Single actors also offer the potential for non-nation state or state actors to exploit an attack. This overlap could be known or unknown to the single-threat actor. But the small opening in NATO defenses could give larger actors a beginning foothold for a larger attack.

Non-Nation State Groups:

A non-nation state group provides a considerable threat to NATO and its members. Because of EDTs, this actor will have nearly the same capabilities as a state actor, and their impact is likely to be significant.

The main weakness they can exploit in NATO is the fact that currently, there are little means to deal with this kind of threat actor. They operate without borders and are untethered from international laws and treaties. This posture creates a beneficial environment for the actor.

One difference between the non-nation state group and the state actors will be their access to a large nuclear arsenal. In the future, it is likely that non-nation state groups will gain access to nuclear materials and a small number of nuclear devices. Even with this, non-nation groups won't have the same tracking and launch technologies as a traditional nuclear weapons state.

State Actors:

State actors pose the greatest and most complex threat to NATO, since they have a clear strategic path that touches all six findings. Russia, China, India, Pakistan, North Korea, and Israel are the most critical to consider because of their nuclear capabilities. Below, we outline how all key findings create vulnerabilities.

- **Finding #1, Geopolitical Conflict**
Escalation: This is most closely tied to the threat of nuclear escalation and is exacerbated by the adoption of EDTs into defense systems, the existence of dual-use vulnerabilities, and industry's strong control over dual-use technology development.

- **Finding #2, Lowering the Bar:** This finding can apply to the actors cited above, especially the countries who may be outmatched in EDT supremacy and see the use of a WMD as their only option. This will also apply to other actors who might gain possession of a single or small collection of nuclear devices, while feeling as if their “back is against the wall”. They may also consider the use of a tactical, single nuclear device as acceptable. The NATO weakness or vulnerability in this instance might be counter-intuitive. The weakness in this case is the strength of NATO members’ EDT arsenal. The EDT supremacy when used against lesser equipped countries could push them to use a nuclear device.
- **Finding #3, New Insider Threats:** Insider threats are a traditional and known attack space for nation states. Nation states will continue to use espionage, counter-intelligence, blackmail, and coercive measures to develop and exploit insider threats within NATO. The new area of interest in this finding includes the speed, scope, scale, and impact an individual can have whether they know they are a threat or not.
- **Findings #4, #5, and #6:** All three of

these findings are influenced by the same weakness. The unmonitored development of EDTs leaves NATO members vulnerable to these attacks. WMD effects will leave NATO unprepared for the combination of EDTs used as weapons or other WMD devices. This type of attack will be particularly attractive to non-nuclear enabled or non-WMD enabled nation states. This will give them an advantage in conflicts

If left unchecked, EDTs will give nation states sizable targets within NATO members’ critical infrastructure. The vulnerability lies in the complexity of each member’s critical infrastructure as well as the lack of definition and tracking across member states. This Destabilization of Critical Infrastructure will also slow down member states’ reactions and could delay the triggering of Articles 4 and 5.

Finally, the Long Game is one of the more complex and subtle threats. It is a threat that does not initially present itself as a threat. If NATO and its members are not prepared, this long game could remain unseen for an extended period of time. Lack of preparedness and monitoring will leave NATO vulnerable to possible multiple attacks of this kind.





DETERRENCE

A NEXT GENERATION OF INTEGRATED DETERRENCE

Definition:

The emergence of EDTs and their use with WMDs will mean that a new approach to WMD deterrence will be needed.

Current State and Strategic Path:

Currently, NATO member deterrence is not sufficient to guard against and prevent the effects of EDTs on WMD and WMD effects. The concept of integrated deterrence, namely as a concerted effort to use all domains, all instruments of national power, and do so with allies and partners to deny scenarios of conflict, is emerging as the latest iteration of deterrence strategy⁷⁶

In the 2022 National Defense Strategy, the United States explicitly calls out integrated deterrence as its strategy to advance national defense goals. As the unclassified version of the NDS is not yet available to the public, it is unclear how the Department of Defense will consider emerging technology threats in its strategy. However, the U.S. strategy includes a goal of “building enduring advantages for the future Joint Force” through “getting the technology we need more quickly”, which implies continuing to pursue research, development, and acquisition of emerging technologies.⁷⁸

NATO has embraced integrated deterrence as a concept, although the organization has not yet committed to it as a strategy. NATO think tanks have studied integrated deterrence and recommend its implementation as an offset strategy or “First Reset Strategy”⁷⁹ Conceptually, integration is vertical, horizontal, functional, and temporal. The goal of this strategy is to “overhaul and re-energise [NATO’s] decision-making processes to be able to react to a fast-breaking crisis anywhere, at any time”.⁸⁰

We concur, and add that reacting to a crisis is only part of the deterrence solution. The concept of integrated deterrence needs to incorporate the emergence of destructive technologies to get ahead of a potential conflict escalation spiral. We have modeled dozens of possible threats that emphasize how EDTs are making weapons of mass destruction more lethal and more accessible. Incorporating a programmatic emphasis on the implications of EDTs is the next step for implementing a sufficient deterrence strategy

76 Garamone, *Concept of Integrated Deterrence Will Be Key to National Defense Strategy*, DOD Official Says.

77 U.S. Department of Defense, *Fact Sheet: 2022 National Defense Strategy*.

78 U.S. Department of Defense, *2022 National Defense Strategy*, p. 2.

79 GLOBSEC Policy Institute, *Integrated Deterrence: NATO's 'First Reset' Strategy*,

80 Ibid, 16.



CONCLUSION

CONCLUSION

Given historical events and future forecasting, it's expected that the world of 2040 will be more unpredictable and unstable with an increased potential for international conflict between great powers. Both China and Russia continue to develop significant military capabilities with the intent to change the current rules-based order of the world. The world is on the cusp of a change in the fundamental character of war.



The nature of war, however, won't change. It is a decision by humans to impose their political will on their opponents by the use of violence. War will still be characterized by "fog, friction, and chance". Its causes will still likely be related to fear, pride, and personal interests. Conversely, the character of war will change (i.e., how and where wars are fought, and with what weapons, technologies, organizations, and doctrine). Namely, the "ways" and "means" of war will change.

Throughout history, we have seen a number of examples of the changing character of war. Consider how the smooth bore musket gave way to the rifle; how communications shifted from guidons to the radio and the internet; and how naval vessels shifted from sails to steam. Moving forward, the next fundamental change in the character of war will be driven by technological innovation and the development of EDTs. In the end, the challenge in every domain of warfare is for NATO alliance members and partners to understand how EDTs affect them individually and collectively. They need to create plans for monitoring and affecting the development and adoption of these technologies, and create strategies that help NATO maintain peace and order.

For NATO members, the ultimate goal should be to deter great power war and maintain great power peace. To be successful, we can't cling to the concepts, weapons, and organizations of the past because they are familiar and comfortable to us. The future battlefield demands more. It will be highly complex, decisive in urban areas with large civilian populations, non-linear, and non-contiguous in time and space. This project was done jointly between the Army Cyber Institute at West Point, NATO ACT, and Arizona State University. Our goal was to examine how the future of 2040 is likely to operate and provide recommendations on how to prepare for, mitigate, and respond to the threats associated with it.



APPENDIX I

EDT EXPLANATIONS

ADVANCED COMPUTING

Advanced Computing is an umbrella term covering emerging or cutting-edge computational technology currently in development. The term can refer to both hardware and software running on these machines. More recently, the term has expanded to include network devices and the hardware and software platforms that connect them. The term itself is intentionally nebulous given the rapid pace of change, as technologies achieve mainstream success or fail to break through.

Currently, Advanced Computing refers to, but is not limited to the following range of technologies:

- Supercomputing, edge computing, cloud computing, storage of “big data”, and new computing architectures;
- Virtual reality (VR), augmented reality (AR), mixed reality (XR), and “the Metaverse”;
- Trusted authentication, disaster recovery, computer forensics, and identity management;
- Digital convergence between cyber and physical systems;
- Blockchains, “web3,” shared distributed edger, traceability, and trustless systems; and
- Neuromorphic, edge, virtual systems, and 5G.

Typically included on this list are also artificial intelligence (AI), quantum computing, and the Internet of Things (IoT). For the purposes of this report, we detail them separately below.

As of May 2022⁸¹, the leaders in Advanced Computing are the United States and China. Many nation-states are leaders or close partners in a particular technology, including India in data science, the UK in blockchains, and South Korea and Finland with 5G.

However, each nation's approach to development differs. The United States, for example, relies on academia for basic research, which is funded by government institutions and non-profit foundations. There, commercialization is ultimately left to private investors and later publicly-traded corporations. China, by contrast, drafts five-year strategic plans including industrial policy, then channels state funding into academic, industrial, and research functions.

ADVANCED MANUFACTURING

Advanced Manufacturing is another broadly-defined term referring to emerging technologies related to manufacturing processes and materials. It is defined by Manufacturing USA as the “use of innovative technologies to create existing products and the creation of new products. Advanced Manufacturing can include production activities that depend on information, automation, computation, software, sensing, and networking.”⁸²

An alternate definition provided by the European Commission's Advanced Technologies for Industries project states that “Advanced manufacturing technology encompasses the use of innovative technology to improve products or processes that drive innovation. It covers two types of technologies: process technology that is used to produce any of other advanced technologies, and process technology that is based on robotics, automation technology or computer-integrated manufacturing. For the former, such process technology typically relates to production apparatus, equipment and procedures for the manufacture of specific materials and components. For the latter, process technology includes measuring, control and testing devices for machines, machine tools and various areas of automated or IT-based manufacturing technology.”⁸³

For the purposes of this report, Advanced Manufacturing includes the following technologies:

- Additive manufacturing, such as 3D printing;
- Smart manufacturing;
- Nanomanufacturing;
- Robotics used in manufacturing;
- Automation technology; and
- Computer-integrated manufacturing.

81 United Nations Conference on Trade and Development, *Technology and Innovation Report 2021*.

82 Manufacturing.gov, *Glossary: Advanced Manufacturing*.

83 European Commission, *Advanced Manufacturing Technology*.

The adoption and sophistication of current Advanced Manufacturing technologies varies worldwide. South Korea, Japan, Germany, Singapore, and Sweden lead the way in robotic manufacturing, for instance, while the United States and China are the clear leaders in additive manufacturing, followed by the UK, Germany, and Singapore.⁸⁴

ARTIFICIAL INTELLIGENCE

The United States Department of Defense, in their 2018 AI Strategy, defines artificial intelligence as “the ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems.”⁸⁵ For the purposes of this report, AI is defined more loosely. In the words of computer scientist Elaine Rich, “AI is the study of how to make computers do things at which, at the present time, people are better”.⁸⁶

There are three main sub-categories of AI. The most common variety today is artificial narrow intelligence (ANI), which some researchers refer to as “weak” AI. These algorithms are goal-oriented and designed to perform a specific task. The “weak” notation is misleading in that the current uses of ANI, while narrow, have proven robust and successful. Some of the more promising examples of ANI include Amazon’s and Apple’s voice assistants, Facebook’s facial recognition abilities, and OpenAI’s GPT-3 and DALL-E 2 – all of which can spontaneously generate creative text and images from open-ended prompts.

Artificial general intelligence (AGI), on the other hand, has been dubbed “strong” AI. This is the domain of machines that learn, understand, and act in ways that are analogous to humans. They are able to think, strategize, and perform multiple tasks under uncertain conditions without a priori knowledge or by being specifically designed to perform them. AGIs do not currently exist, but predictions of their imminent arrival have been a hallmark of the field.

Artificial super intelligence (ASI) is a hypothetical goal seen most often in science fiction films and novels. These are machines that have transcended sentience and are capable of genuine creativity, social skills, and wisdom.

For the purposes of this report, AI as an EDT includes the following sub-fields and related technologies:

- Machine learning;
- Deep learning;
- Reinforcement learning;
- Sensory perception and recognition;
- Next-generation AI;
- Safe and/or secure AI; and
- Human-machine teaming.

As of May 2022, the U.S. Congressional Research Service assessed that narrow AI was fully or partly incorporated into military applications, such as: intelligence, surveillance, and reconnaissance (ISR); logistics and supply operations; cyber operations; autonomous and semi-autonomous vehicles; and command and control functions.⁸⁷ Training a narrow AI requires large datasets, and the process still struggles with opacity, training bias, and lack of resiliency. For example, many AI applications, such as image recognition can be fooled with small data changes imperceptible to the human eye.

China is the closest peer competitor to the U.S. in AI, having already developed sophisticated language- and facial-recognition technologies for its domestic surveillance network. AI-enabled autonomous swarm research and cyber operations are at the top of the list of its ongoing R&D efforts.

Similarly, Russia seeks to arm at least 30% of its military equipment with AI-powered robotics in the next five years, including research into ground-, aerial-, undersea-, and naval-swarmling. Russia's AI research also prioritizes propaganda, misinformation, and information warfare efforts against the United States. Part of this effort may be directed at improving "deepfake" creation and distribution.

AUTONOMOUS ROBOTICS

"Autonomy" is the ability to independently decide and act. In robotics, autonomous systems are able to perceive their environment, make decisions based on that data, then perform an action, such as a movement or object manipulation accordingly — all without human intervention.

For the purposes of this report, the following sub-components fall under the heading of Autonomous Robotics:

84 United Nations Conference on Trade and Development, *Technology and Innovation Report 2021*.

85 U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, 5.

86 Rich, *Artificial Intelligence and the Humanities*.

87 Sayler, *Emerging Military Technologies: Background and Issues for Congress*, 2-8.

- Surface;
- Air;
- Maritime;
- Space;
- Swarms;
- Weapons platforms; and
- Uses in civilian critical infrastructure.

In 2020, the International Federation of Robots ranked Singapore, South Korea, Japan, Germany, Sweden, Denmark, Hong Kong, Taiwan, the U.S., Belgium, and Luxemburg as the world's most automated countries.⁸⁸ That year, average manufacturing robot density hit a new global record of 113 units per 10,000 employees. Regionally, Western Europe (225) and the Nordics (204) have the highest density, followed by North America (153) and Southeast Asia (119).⁸⁹

Top global manufacturers of industrial robots include ABB (Switzerland), FANUC (Japan), KUKA (China), Mitsubishi Electric (Japan) and Yaskawa (Japan). Leading manufacturers of humanoid robots include Hanson Robotics (Hong Kong, China), Pal Robotics (Spain), Robotics (South Korea) and Softbank Robotics (Japan).⁹⁰

In terms of research, the United States, China, and Japan have published the most scientific papers, while the U.S. has a dominant lead in patenting, followed distantly by South Korea and Germany.

BIOTECHNOLOGIES

As its name indicates, biotechnologies use cellular and biomolecular processes to develop new technologies and products in agriculture, health, energy, and more. The goal with this technology is to create biological factories that can be reprogrammed to produce tailored outputs, which include biological weapons.

For the purposes of this report, biotechnologies include the following components:

- Synthetic biology;
- Genome editing;
- Emerging pathogens detection and characterization;
- Engineering of viral and viral delivery systems; and
- Biomanufacturing and bioprocessing technologies.

Recent game-changers in the biotechnologies threat space include the increasing availability of gene editing techniques, the falling costs of gene sequencing, and the

worldwide response to COVID-19 – all in terms of detection, vaccination, and other protective measures.

Experts are divided on whether virology and genetic-manipulation techniques will mature quickly enough and at a sufficient scale to be a significant concern by 2035. While COVID-19 may have led to an unprecedented degree of interest and funding in these fields, including the rapid development, manufacturing, and distribution of novel mRNA vaccines, we predict that within a decade, funding, attention, and institutional knowledge may dissipate, providing an adversary the opportunity to strike with a biological threat.

The Institute for Defense Analyses assesses that the U.S. efforts in biotechnology have historically been developed in the private sector as a civilian or economic pursuit.⁹¹ In the U.S., the biotechnology industry amounts to between 5%-7% of the U.S. GDP, and it is growing around 10% annually, according to the U.S. National Academies of Science.⁹²

CYBER

Cyber has continuously had a fluid meaning with beginnings in Norbert Weiner's pioneering work with cybernetics in the 1940s through further development by such people as science fiction author, William Gibson's, coinage of "cyberspace" in the 1980s.

This report uses the U.S. military's definition outlined in Joint Publication 3-12, which refers to it as "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."⁹³

This definition of cyber focuses on the use of that domain as a platform and staging area for attacks on enemy systems. For example, in a 2015 hearing of the U.S. House Committee on Foreign Affairs, James A. Lewis, director of the Strategic Technologies Program at the Center for Strategic and International Studies, explained cyber as "the ability to remotely manipulate computer networks...The Internet and computers provide cyber tools and techniques that countries use for influence, coercion and, potentially, attack. Militaries will use cyberattacks to disrupt command and control, manipulate software, degrade weapons performance and produce political or psychological effects."⁹⁴

88 International Federation of Robotics (IFR), *Robot Race: The World's Top 10 automated countries*.

89 Ibid.

90 United Nations Conference on Trade and Development, *Technology and Innovation Report 2021*.

91 Carlson, Robert, Sbragia, and Sixt. *Beyond Biological Defense: Biotech in U.S. National Security and Great Power Competition*.

92 Ibid.

93 Joint Publication 3-12, *Cyberspace Operations*.

94 U.S. Congress. House and Committee on Foreign Affairs, *Cyber War Definitions, Deterrence, and Foreign Policy*.

95 Voo, Hemani, Jones, DeSombre, Cassidy, and Schwarzenbach, *National Cyber Power Index 2020*.

Cyber threats typically do not produce destructive effects similar to WMDs or kinetic weapons, but instead seek to disrupt data and communications, create confusion, damage networks and computers, and destroy machinery. Significantly, these attacks are also targeted at military and government targets as well as critical civilian infrastructure, such as was the case with Russia's successful attack on Ukraine's power grid in December 2015.

For the purposes of this report, cyber threats, attacks, and warfare also include the following components:

- The use of and attack on computer hardware, software, and networks;
- An attack on government, military, industrial, and public networks and data;
- The disruption and destabilization of infrastructure, commerce, and civilian psychology; and
- Compromising cloud service providers, managed service providers, other third-party data hosting providers, or supply chain attacks.

Harvard's Belfer Center for Science and International Affairs has developed The National Cyber Power Index (NCPI), measuring 30 countries' cyber capabilities in the context of seven national objectives, using 32 intent indicators and 27 capability indicators with evidence collected from publicly available data. The United States is at the top of the list, followed closely by China, the United Kingdom, and Russia.

INDUSTRIAL INTERNET OF THINGS

The Industrial Internet of Things (IIoT) is the subset of the Internet of Things (IoT) focused on critical sectors and infrastructure. It represents a technology stack that combines sensors, local bandwidth, data storage and processing, real-time analytics, and control systems. The difference between IoT and IIoT is that attacks on and system failures by the latter can result in life-threatening situations and potentially mass casualty events.

For the purposes of this report, we are most interested in the application of IIoT in the following areas:

- • "Smart cities" and public-private infrastructure;
- • Government and municipal infrastructure; and
- • Manufacturing and supply chains.

The national leaders in general IoT deployments, as measured by spending, is the United States, China, Japan, and Germany.⁹⁶ In 2021, a report funded by the Netherlands Ministry

of Foreign Affairs found that “the European market for Internet of Things (IoT) solutions is growing. Germany, the United Kingdom, France, Italy, Spain and the Netherlands are leading European IoT adoption, but Eastern European countries and the Nordics are following closely.”⁹⁷

A review of the “state of the art” in IIoT found it in use across multiple sectors, including “environmental monitoring, agriculture, construction, smart homes and buildings, disaster management, smart grids, robotics, health care, automotive industries, and emergency response systems.”⁹⁸

HYPERSONICS

Hypersonics are ballistic weapons capable of flying at a minimum speed of Mach 5. Unlike traditional ballistics, which follow a steady trajectory that enables the calculation of their targets, hypersonics are able to maneuver in mid-air. This ability significantly complicates attempts for both interception and evasive action. To date, there are no defenses against hypersonics, and some experts question the technical feasibility of creating one.

There are two sub-classes of hypersonics, each with distinct characteristics. The first is a hypersonic glide vehicle (HGV) launched from a ballistic missile or rocket booster. The Congressional Research Service (CRS) notes HGVs are steerable, normally detached at a lower, flatter trajectory than ballistic payloads, and as a result makes it difficult to predict the flight path.⁹⁹ The United States is currently not developing HGVs for use with nuclear warheads, although Russia and China likely are.¹⁰⁰ The CRS also assesses that Russia and China are building HGVs with the intent to meet their nation’s security interests, not to compete with the U.S. development of HGVs.

The second sub-class are hypersonic cruise missiles (HCM) that rely on air-breathing scramjet engines to accelerate to hypersonic speeds at the edge of Earth’s atmosphere. The scramjet engine operates after the weapon has been launched from a traditional booster or bomber, before accelerating to hypersonic speeds. HCMs are also maneuverable and capable of evading layered ballistic defenses.¹⁰¹ HGVs and HCMs primarily differ on their launch mechanisms and glide angles, but there are also technical aspects at play.

96 Statista, *Forecast Internet of Things (IoT) spending worldwide in 2019, by country*.

97 CBI, *The European market potential for (Industrial) Internet of Things*.

98 Malik, Sharma, Singh, Gehlot, Satapathy, Alnumay, Pelusi, Ghosh, Nayak, *Industrial Internet of Things and its Applications in Industry 4.0: State of The Art*

99 Saylor and Woolf, *Defense Primer: Hypersonic Boost-Glide Weapons*.

100 Ibid.

101 Missile Defense Advocacy Alliance, *Hypersonic Weapon Basics*.

For the purposes of this report, hypersonics refer to the entire system and supply chain supporting the development and deployment of hypersonic weapons. This includes, but is not limited to:

- Propulsion systems;
- Aerodynamics and control;
- Materials;
- Detection, tracking, and characterization; and
- Defense.

The Switzerland-based Center for Security Studies has determined that both “Russia and China are motivated to acquire hypersonic weapon capability not only to have more long-range missiles and better nuclear deterrence, but also for their tactical use in a naval contest, especially anti-ship missiles that can sink aircraft carriers.”¹⁰² This means that hypersonics research and development are more encompassing than just replacing first-strike nuclear intercontinental ballistic missiles.

The U.S., China, and Russia are leading hypersonic weapons development, while Australia, Japan, Germany, India, South Korea, North Korea, and France are also developing hypersonic weapons technology. Several of these countries, including France and China, are collaborating with Russia.¹⁰³

In the United States, the Navy, Air Force, Army, and DARPA are engaged in no less than seven major hypersonic weapons and hypersonic technology programs estimated at over 3.2 billion USD (in 2021).¹⁰⁴ None of these systems are yet programs of record, although prototypes demonstrating various modes of employment (e.g., missile launched, sea-based, air breathing, and low orbit technologies) have been in development for decades.¹⁰⁵

According to the U.S. Congressional Research Service, Russia’s hypersonic program includes two true hypersonic weapons (the Avangard and the ship-launched Tsirkon) and one “maneuvering air-launched ballistic missile” (the Kinzhal) that poses similar defensive challenges.¹⁰⁶ The Avangard currently rides on the SS-19 Stiletto ICBM and has been successfully tested in 2016 and 2018. Russian news claims the Avangard has been cleared for “combat duty” in December 2019. Russia plans to move the weapon to the Sarmat ICBM in the future. The Sarmat was last successfully tested in April 2022 and reportedly can carry three Avangard glide vehicles.¹⁰⁷

China is researching hypersonic glide vehicles and has successfully tested both the DF-ZF and the Starry Sky-2. China is also currently developing at least three other hypersonic vehicle models: D18-1S, D18-2S, and D18-3S. Their investment in hypersonic research

includes at least 18 wind tunnels under control of the China Aerodynamics Research and Development Center, another three hypersonic wind tunnels ran by the China Academy of Aerospace Aerodynamics, and the country is building the JF-22 wind tunnel expected to facilitate testing up to Mach 30 by 2022.¹⁰⁸

QUANTUM INFORMATION TECHNOLOGIES

As the name indicates, quantum information technologies harness the unique properties of quantum mechanics for computation. In classical computing, a bit representing a 0 or 1 is the smallest unit of information, with long strings of bits compiled to create executable code. In quantum computing, by contrast, a “qubit” can simultaneously exist as either a 0 or 1 or both, which is a state known as superposition.

Adding qubits produces an exponential growth in computing power that can quickly outstrip classical computers in several critical areas, such as factoring large integers, but with physical limitations. Silicon-based computing, on the other hand, operates in many environmental conditions. Qubits can only maintain superposition when cooled to fractions of a degree above absolute zero, which in turn requires complex and bulky refrigeration techniques.

For the purposes of this report, the definition of quantum information technologies includes the following components:

- Quantum computing;
- Materials, isotopes, and fabrication techniques for quantum devices;
- Post-quantum cryptography;
- Quantum sensing;
- Quantum communication; and
- Quantum networking and the Quantum Internet.

Since 2019, the U.S. National Defense Authorization Act (NDAA) has allocated research funds to establish and expand quantum research programs. The U.S. Navy and U.S. Air Force have each designated their respective service research laboratories as a Quantum Information Science Research Center, while the U.S. Army has declined to designate a research center at this time.

¹⁰² Ibid, 3.

¹⁰³ Tiron, *Hypersonic Weapons: Who Has Them and Why It Matters*. See also: Saylor, *Hypersonic Weapons: Background and Issues for Congress*.

¹⁰⁴ Kunertova, *Weaponized and Overhyped: Hypersonic Technology*.

¹⁰⁵ Ibid.

¹⁰⁶ Saylor, *Hypersonic Weapons: Background and Issues for Congress*.

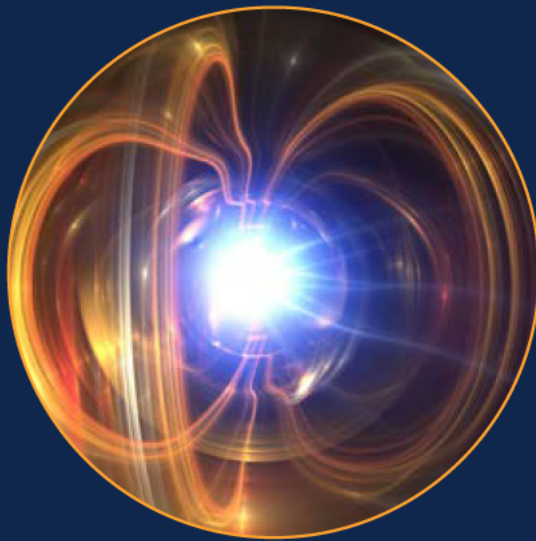
¹⁰⁷ Ibid.

¹⁰⁸ Ibid.

The NDAA also directs the DoD to conduct quantum technology risk assessments, and to extend incentives to high school STEM programs to include quantum information sciences in their programs. Since the majority of quantum research in the U.S. is done through the private sector, the NDAA also directs DoD to improve partnerships with small and medium enterprises on the leading edge of quantum R&D.

Elsewhere, both China and Russia have implemented formal programs to develop quantum capabilities. In 2016, China launched the world's first quantum satellite, Micius, to study space-to-ground encrypted quantum communications. China has also invested in a terrestrial quantum communication network more than 1,250 miles long. The Congressional Research Service assesses that Russia is at least five to 10 years behind the U.S. and China in quantum research, but the country has allocated nearly \$800 million to achieve toward its goals in the Russian Quantum Technologies Roadmap.¹⁰⁹ Most of both of these countries' efforts are led by their respective governments.

Other entities that have made significant quantum investments include the U.K., Canada, and European Union. The latter's program has allocated \$1.1 billion over a decade to commercialize quantum advances.¹¹⁰ Australia, Germany, Netherlands, and Austria have made similar, but smaller investments.



109 Saylor, *Emerging Military Technologies: Background and Issues for Congress*, 24-26.

110 Moloney-Figliola, *Quantum Information Science: Applications, Global Research and Development, and Policy Considerations*, 9.



APPENDIX II

SUBJECT MATTER EXPERT TRANSCRIPTS

MELANIE W. SISSON

Melanie W. Sisson is a fellow in the Foreign Policy program's Center for Security, Strategy, and Technology where she researches the use of the armed forces in international politics, U.S. national security strategy, and military applications of emerging technologies.

Hi, my name is Melanie Sisson. I'm happy to be joining you today from the Brookings Institution's Talbott Center for Security, Strategy and Technology, where I'm a fellow and to present to you some research done on anticipating the effects of emerging technologies on nuclear deterrence.

I've put on the slide here, the specific prompts that were addressed in this research. And I do that both to orient us into the questions, but also so that I can point out that the questions are really very direct. And then also to note that I've tried to answer them equally directly. One other item as we get started, and this one is definitional. Throughout, when I refer to artificial intelligence, I'm including advanced computing for purposes of managing, processing and analyzing large volumes of data and machine learning, but I'm not including general sentience. And when I refer to cyberspace, what I mean is systems of digital connectivity that move data between and among electronic devices.

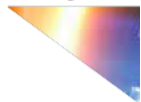
To consider how emerging and disruptive technologies or EDTs will affect state's nuclear strategies - we have to begin by understanding what it is nuclear strategy is intended to achieve. Since 1954, the United States has designed its nuclear strategy to deter the use of nuclear weapons on itself and its treaty allies. And since 1967, also to deter conventional attacks. Because we're in a world where other states are nuclear armed, effective deterrence requires two things: a nuclear arsenal and secure second strike capability. In other words, for nuclear deterrence to be effective, nuclear armed competitors must all believe that each can absorb a first strike and still return nuclear response. Effective nuclear deterrence in this way create stability - a condition under which nobody has an incentive to strike first because there's no first mover advantage to be had. Stability is achieved, in other words, when all nuclear states recognize that nobody

wins and everyone loses in a nuclear exchange. To date, states have achieved second strike assurance by hiding and defending a subset of their nuclear arsenals by using harden missile silos, rapid launch and dispersal, mobility, and the oceans.

Emerging technologies are degrading the effectiveness of these approaches. There are more and more usable technologies that make more of the world more observable more of the time. There are more and more usable technologies that make data more plentiful and more useful. And there are more and more usable technologies that enable more devices to act on the world independently of human intervention. As these technology advance over time and as their potential is realized through integration, and here I'm thinking of uncrewed platforms powered by compact and durable energy sources that are equipped with high fidelity sensors and edge computing, including artificial intelligence, their applications for purposes of intelligence surveillance and reconnaissance or ISR will increasingly allow all states to better identify, monitor, track, and target nuclear assets. This can happen intentionally and/or it also can happen as a byproduct of deployments that are designed to acquire information for other purposes. Movement in this direction is ongoing and as the United States and competitor militaries continue to modernize - it increasingly will challenge secure second strike, terrestrial hiding will become increasingly difficult to achieve, and the oceans also eventually will, as the saying goes, become more transparent.

Defending nuclear assets also will become more difficult. In the first instance, hardening isn't really a match for mass bombardment and to the extent that rapid launch relies upon nuclear command control and communication systems or NC3, its integrity no longer can be guaranteed. Advances in artificial intelligence are creating strategic risks in cyberspace, which I usually characterize as the wild west of interstate interaction today. Cyberspace is decentralized, it's everywhere at all times, it can be accessed by anyone and it's bidirectional. Devices can receive and can push data. These features mean that insertions of digital code that instruct devices to behave in particular ways can achieve a multitude of adversarial cyber effects, including espionage, but also data corruption and system disruption. NC3 is composed of technologies that sense, process, analyze, visualize, and distribute digital information that enable communication and that power, those functions. And these systems are far from immune from cyber attacks. In addition to creating risks of nuclear accidents and unintended launches, the possibility of adversarial intrusions into NC3 by state or non-state actors could make it possible to disable launch or to redirect targeting. If an actor were to believe it had achieved a disabling or diverting cyber attack on an adversary's NC3, secure second strike assurance would dissolve and nuclear deterrence would go with it. As with ISR, this outcome could occur either intentionally or as an unintended result of system intermingling.

I noted before that the United States and its nuclear armed competitors will pursue EDTs and systems of EDTs. And so all of them also should be expected to seek ways to counter the effects of those tools and systems as they seek to ensure the survivability of their



nuclear assets. China, with its limited arsenal, has the most reason to make adjustments of scale. In particular, by establishing a robust nuclear triad. The United States and Russia already have ample stocks of warheads and delivery systems and well-established triads. For these countries, advances in ISR will increase the value of mobile air and sea-based nuclear capabilities with ocean hiding remaining the most viable for the longest period of time. Investments in land-based Intercontinental ballistic missiles or ICBMs by contrast, and especially those in silos, can be argued to be useful for deterrence generally, but they are not meaningful responses to emerging technologies. The great equalizer, unfortunately, is in cyberspace and here all states and not just those with their own nuclear assets, have reason to invest in offensive and defensive cyber capabilities that could be deployed against NC3 systems.

I think that advances in ISR will create nuclear instability in the medium term. I think terrestrial hiding and evasion through air mobility will become less possible relatively quickly, and that sea-based nuclear assets will retain their currency longer, but not indefinitely. My guess is that the nature of technology and technology transfer means that states generally will make synchronous progress, but it's possible that one actor will jump out ahead or will think that it has jumped out ahead or that others will think that it has jumped out ahead. Any of those outcomes will degrade stability by either actually or simply seeming to create a first strike incentive. Even more concerning are the near-term risks in cyberspace. By near term, I mean now - today, as reports make clear that states are actively undertaking cyber operations on each other's nuclear infrastructure. Cyber defenses will never be impenetrable, and the risks posed by ISR, can't be addressed adequately through adjustments to nuclear posture. This means that achieving the next nuclear equilibrium will require coordination of behavior. States will have to agree to do and not to do certain things. This means that the United States needs to seek to engage China and Russia in conversations that will lead to the development of mutual approaches to risk reduction. I'm not suggesting that this will be straightforward or easy. I am just saying that it is necessary.

I think we can take some lessons from the cold war experience of arms control though. Of course, the trick will be to adapt them to the new environment, to new technologies and to new partners in China and Russia. Given the tenor of the U.S. relationships with those states today, simply creating lines of communication and giving them a few repetitions will be as important and possibly even more important in deciding which specific risks to address first. If we need to choose one, it won't surprise you that I'd suggest beginning with making any progress we can prohibiting the use of AI enabled technologies in cyberspace to attack the nuclear enterprise.

I'll finish with one note about the DOD China military power report, because it contains an important section on China's nuclear activity. I've heard and seen commentary suggesting that China's expansion of its nuclear arsenal and development of its triad might indicate a shift away from its long time, No first use policy. This of course is possible, but it's only

one of a number of possible explanations. China might be seeking nuclear parity, for example, because it believes this will reduce its vulnerability to nuclear coercion. It might also be anticipating the effect of emerging technologies and taking steps to increase the survivability of its arsenal. And there might be other reasons. China's capabilities bear close monitoring, no doubt, and so does its intent. But we would do well to remember that understanding intent requires more than measuring capability. This is always important, but I think especially important when it comes to nuclear strategy where the risks of arms racing and the security spiral are pronounced and the consequences of getting it wrong are so severe.

JOHN ARQUILLA

John Arquilla is Distinguished Professor Emeritus of Defense Analysis at the U.S. Naval Postgraduate School. He is best known for developing the concept of cyberwar in the early 1990s, and continues to contribute to the cyber discourse, most recently in his Bitskrieg: The New Challenge of Cyberwarfare (Polity, 2021). Dr. Arquilla is presently working on a study of the implications of advances in artificial intelligence for military and security affairs.

Thank you so much, Colonel, for this opportunity to share a few thoughts with you on these cyber issues and how they relate to weapons of mass destruction, and what I call mass disruptive weapons as well. I think there are several topics here that might be of interest to those in your program.

The first is basically to have a realization, as many hackers do, by the way, about the complexity of cyberspace. One really doesn't know for sure, even if one tries to target very carefully a specific kind of equipment or a system, you don't really ever know what's exactly going to happen. And for me, a good example of this is when an autistic young man from Britain who was interested, about 20 years ago, in finding out information about UFOs and he thought the best place to go for that would be to search in the U.S. Air Force files. So, he hacked in and while looking for information about UFOs, he just happened to trigger a virus that shut down air defenses along the east coast and without any intention of doing so, it also knocked out the supply and logistics system supporting the Atlantic fleet. So, that's just an example of how you might aim to do one thing and other unexpected things happen. This occurs as well in my book, Bitskrieg, which is a latter-day analogy of the Blitzkrieg, the great military doctrine of the 20th century. Bitskrieg, that is using bits and bytes to guide the bombs and bullets, will have, I think, a similar profound effect on military affairs in the 21st century. But I use other examples, some of the early Russian cyber attacks aimed at the Ukraine years ago knocked out port facilities in Italy and other countries for appreciable periods of time.

One has to be aware of and to respect the complexity of cyberspace. I think hackers

also find, even the black hat hackers, are drawn to cyberspace because of its beauty and complexity. It is a wilderness of its own - that has its own sort of charms. And they're drawn to it, some to do bad things and others to be helpful. And, of course, one of my other crusades has been to try to encourage more active recruitment of the master hacker community as other powers are doing. In fact, there's kind of an organizational race to go right along with the arms races underway in the world, and that organizational race is to build hacker networks and China, Russia, and other powers are doing that. The United States, not so much yet. We're more interested in incarcerating hackers and I really think we need to take a long second look at that. We do have some people with non-regulation haircuts and body piercings in various units and commands here and there. But not enough. That's the other problem. We have to be able to bring in people who can't be vetted for a security clearance or might not meet physical standards of military service.

Anyway, then the takeaway is this complexity means that we have to be prepared, when we use cyber abilities, for unintended effects to arise. I guess we could call it a kind of collateral damage that may occur. We also have to be aware that when our own systems are targeted, we have to be ready to respond and reconstitute when unexpected things happen like that knocking out of air defenses on the east coast and the Atlantic fleet supply. So, reconstitution is probably something we need to be aware of.

The corollary point here is that the more advanced the technologies of any military, the more vulnerable they are to disruption. This is very different from the industrial age where, you know, when you had a lot of tanks and a lot of artillery, you had a lot of power. The more you could produce, the more power you had. The United States, after Pearl Harbor, had a lot of its battleship fleet disabled, had a couple of carriers, realized that the aircraft carrier was, through air power, now the key to Naval power. And so, we built another hundred of these over the course of the rest of the war. Production and power went hand in hand. But in an information age, the very things that make you more powerful also make you more vulnerable.

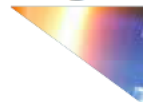
And this I think is a great area of concern. It put an absolute premium on strongly defending the advanced communications, sensing, information and management control systems that modern militaries rely so heavily upon. So, hold on to that thought as well, that now power and vulnerability go hand in hand. And this goes not only for national military forces, but also for the very prosperity of a nation. The more reliant it is on advanced technology, the more vulnerable it is to disruption. And for the United States, this is an even more complicated problem because a lot of our infrastructure pipelines and such - we know from the Colonial Pipeline incident, a lot of that infrastructure was put in place prior to web and net connectivity. Yet they're all connected to the web and the net in ways that make them vulnerable. So, this Colonial Pipeline built in the 1960s with the most advanced software that could run it was from the 1970s. At the time of the incident, that was very easily hackable and created a mass disruptive event along the Eastern seaboard of the country.

The other thing I would say, and I'm sure all in the cyber business know this already, is about the veil of anonymity that often enshrouds the cyber malefactor. And, even when we think we have good forensic evidence, bad guys can always say, "we didn't do that" or "we had no idea that people were using our territory to do bad things". What this means is that our ability to deter, particularly by means of retaliatory threats, is really terribly impeded. And the attempt to use, as has been the case in cyber for quite some time, to use the paradigm from the physical world about punitive deterrence, or even denial deterrence really doesn't work in cyberspace.

So, we have to think in other terms. I think the simple answer is we have to get a lot better at defense of our systems. And when I say systems, I mean, soup to nuts, not just the combatant commands, the field services, but space systems (those that are very reliant on cyber) and of course ground stations can be hacked. And, so we have to worry about that. And there's even been some interesting work done on the vulnerability of command and control systems for our nuclear arsenal. Of course, the Russians have always worried about this. They've had a "dead hand," automated system for their nuclear command and control for several decades. And in fact, that was a system built again before web and net connectivity. And, can't say more about their command and control, but they too have concerns about these areas.

And if you can't deter the bad guys, you must shift to defense. Now, some talk in terms of forward defense, the idea of preemptive actions – striking when under threat of imminent attack – that's gonna be very, very hard. It's hard to figure out when an attack is coming, in part, because they come out of the blue. A lot of the time in other areas where we know intrusions are being made, often those are intelligence gathering and what a hacker does to gain access, to be able to gather intelligence is observationally equivalent to what they would do to get into a system and lay sleeper weapons, or prepare for an actual cyber attack. So that's a very, very, very tricky business for preemption.

That leaves basically prevention action as our go-to strategy. And part of that prevention is to use very strong encryption in what I call in, in my book, data mobility. Move things around, don't just put 'em in the cloud. Remember that the cloud is just someone else's computer, but the good news is it is somewhere else. And so you put it out there. Take your really valuable information, put it out there in a strongly encrypted way. In fact, maybe even break the document up into several pieces, put it in different parts of the cloud. You're making the business of the Hacker that much harder. And this, by the way, is good advice for commercial enterprises as well. I just saw the figures for 2021. It looks like intellectual property theft cost in pirated and counterfeit goods and also in competitive industrial areas where industrial secrets have been leaked out - the figure they give for that is a cost of \$2 trillion. Which is, you know, somewhere around 4 or 5% of global economic product is being bled out through what I call in the book, strategic crime. Anyway, gotta move things around, gotta keep things more strongly encrypted. This works for individuals, institutions, commercial concerns and, of course, the military. I'm happy to say the



Navy, with which I'm most familiar, has been moving very, very much more toward cloud computing. Just remember this: data at rest are data at risk. So keep it moving - just like in many tactical situations, you know, if you get ambushed the answer isn't to hunker down under the Humvee - it's charge in the direction of the ambush. You gotta keep moving if you're gonna deal with the problem.

In terms of some of the technological issues, 3D printing is something that we have to keep a close eye on. The sophistication of this is increasing by leaps and bounds; And I think they're getting close to an inflection point in terms of the ability to fabricate almost anything except fissile material. And here's where advanced technology and proliferation kind of come together where it looks like we're getting perilously close to a situation where a proliferator can fabricate everything except the fissile material, in terms of putting a weapon together. And by the way, I am critical of our ability to deter cyber action, but I think deterrence (at a nuclear level) is still working reasonably well. That's in terms of weapons of mass destruction, we know that they hit us, we hit them, nothing's gonna be left but the cockroaches and maybe Cher – because nothing can destroy Cher in my personal view. Which reminds me these comments are my views alone and do not represent official defense policy - as if there could be any question about that.

In any event, the technological advances being made (including artificial intelligence technologies) are lowering the barriers to proliferation, and this is going to have some negative effect, I think, on keeping the nuclear club smaller as the years go by. In fact, one has to think about the nuclear club as it is today and realize that our old calculations about nuclear deterrence don't really count anymore. We don't lie awake at night, worrying that Russians have several thousand nuclear warheads, but we're very concerned that North Korea has a handful of them that might actually work and that Iran might get a few. There's a whole new calculus of nuclear deterrence, and it's not so much that we fear that Iran or North Korea would launch a nuclear assault on Los Angeles, or some other city or valued area or ally or friend. It's that they can use the threat of nuclear escalation to support other kinds of aggression. Right? When, when we think of Saddam Hussein taking Kuwait in 1990, we knew we were gonna put a coalition together and push him out. He didn't have a nuclear escalatory capability to threaten our attempt to intervene. One of the reasons we're saying up front that we won't fight the Russians directly if they invade Ukraine is because they are a nuclear power. And we don't want "The Guns of August" this time around to be nuclear guns.

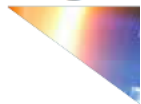
So, the point here is at even a small nuclear arsenal that a North Korea and Iran or some other power might have, could give them a free rein for limited aggression, much as Russia can and China may, when it comes to Taiwan. They might pull the same sort of thing - some kind of limited, conventional aggression, buttressed by nuclear capabilities. (Note: Subsequent to this interview, Putin brandished his nuclear weapons capability to threaten against further NATO support for Ukraine). And it seems to me that that's a whole new deterrence calculus. And it's one of the ways in which nuclear weapons, even

in small numbers can undermine conventional deterrence. So this is a significant problem that we all need to think about. And it may raise the importance of gaining a capability to disrupt nuclear command and control by cyberspace-based means. And I'm sure all sides, in the nuclear competition, are thinking about that.

So, we've got this issue of the shadow of mass destructive weapons is still out there, but they're really hard to use directly and deterrence is reasonable, but we have this whole new range of mass disruptive weapons: the Stuxnets, the Tritons, the various Shamoons, et cetera, a lot of mass disruptive weaponry that's out there and deterrence is very, very poor. And again, this just comes back to my point that we've gotta get a lot better at defense, because deterrence is not something we're going to be able to rely upon.

I've talked a little bit about 3D printing. I think it's also important to speak to the issues that come out of the advances in so-called artificial intelligence. I prefer to think of it simply as silicon-based intelligence, rather than calling it artificial. You know, we're human beings, we are carbon-based intelligence, but silicon-based intelligence is coming. And I think it's going to transform military and security affairs in the 21st century, the way the aircraft transformed Land and Naval warfare in the 20th century. Now what's going on here? There clearly is an arms race underway where both China and Russia (authoritarian societies) have said, we're gonna invest heavily in this, we're gonna have smart hypersonic missiles, we're gonna have tele-operated as well as automated ground combat systems and such. And the liberal societies of the world are behind the curve on this, partly because of concerns of an ethical and legal nature. Some of you are probably aware that the United Nations has an entire initiative on the outlawing of lethal autonomous weapons systems. So it's slowing the process. It's not helped by people like Elon Musk who says that the robots are gonna attack us if we build them. And even the late Steven Hawking joined that club as well. I'm more in the Michael Crichton club – he wrote a wonderful book about electronic life a long time ago in which he said those fears are largely unjustified. I tend in my book to agree with Crichton, and discussed this to some extent.

Well, look, we in the liberal societies aren't gonna get around our ethical and legal and other discourses. We're gonna have to operate within them and move ahead and advance with them. The best I can suggest is that in cyber defensive operations, we need AI to be able to work autonomously. The pace, the tempo of operations can be incredibly fast, beyond human operators' capabilities. So when we're defending, probably should allow full automated systems to work. When we decide to do something offensively, let's keep humans in the loop. I think that's a good compromise for now, moving ahead. But one thing we know for sure is that AI makes a big, big difference. And I would harken to the December 2019 exercises at Fort Benning in which an opposing force is up against a much larger, almost divisional size force. The smaller force was less than a brigade. And, they didn't have automated weapons. What they had was a fully automated ISR system, which allowed them to gain, gather, distill, distribute, and act upon information much more swiftly than in the larger force – and they absolutely destroyed the larger force. You can



probably get some unclassified analyses of the Fort Benning experiment. It is one of the most telling examples of the power of AI.

Another interesting case, this time for aviation enthusiasts - is that the best Top Gun pilot was put up against an AI pilot. They flew two simulators of the same aircraft, did five dogfights and the robot shot down the human pilot each time and in all five dogfights, the human pilot did not put even a single hit on the AI's plane. So, what that says to me is we need to be thinking about units of the 21st century that blend humans, intelligent machines, and probably tele-operated systems. Think of a squadron or an air wing that mixes these in, think of ground forces that have this similar kind of mix, same thing with Naval forces. And I think that's gonna be the great challenge.

I don't have concerns about actual war fighters being reluctant to rely upon or work with robots. What we see is, people love their cars and such, we love our machines already. They're gonna get along well with their bots. In fact, I have some pictures of American soldiers, burying and giving decorations to their AIs or tele-operated systems that have been destroyed in combat. And there's one that's even on display in the iRobot museum up in, I think it's Medford, near Boston. It's this kind of integration of humans and intelligent machines that I think is gonna be the key. And my guess is that this kind of skillful blending is going to be even more effective than a force that would be of just intelligent machines. We shall see, but that would be my prediction.

I think in the interest of time, someone said that it's hard for people to pay attention to anything once a talk goes beyond 10 minutes. So, I think I'm already past that by a little bit. The TEDx people say that 18 minutes is the limit. I may be a little closer to that. So let me just close by suggesting that the era into which we're moving is one of tremendous opportunity, but also of considerable challenge. We tend, when we think about cyber, always to focus first on the issues of vulnerability. Let us also seize upon opportunity, the opportunity for military transformation, the opportunity to build truly strategic defenses. We never succeeded really in the strategic defense initiative that worked against nuclear weapons, but we have a really good chance for a new SDI: a strategic defense initiative for cyber. And that should be on our agenda as well.

Hang onto these notions of complexity, of power and vulnerability going hand in hand. And just as a last thought, I reread *The Guns of August* recently, which if you haven't read it before it's about the crisis of 1914 and why a massive war erupted (that nobody really wanted - they wanted a nice limited war to punish the Serbs) - they got a big war instead. Things got outta control in August 1914 in the Balkans. I think in some respects, cyberspace is the new Balkans. President Biden put it well in a speech he gave last November, in which he said, "if we're going to get into a real shooting war in the future, it's probably going to start by some serious incident in cyberspace". And I think there's so much capacity for mischief-making in cyberspace. I think the President's intuition is probably right and so we have to watch carefully. It's one of the reasons we have to

emphasize building those good defenses. Cyberspace may indeed be the latter-day Balkans. So let us hold that in mind. And, with that, I want to thank Colonel Vanatta for offering me this wonderful opportunity to share some thoughts and let me wish all of you, every success in your endeavors. Thank you, over and out.

SARAH JACOBS GAMBERINI

Sarah Jacobs Gamberini is a Policy Fellow at the National Defense University (NDU) Center for the Study of Weapons of Mass Destruction (CSWMD). Her research and policy support includes emerging technologies, arms control, influence operations, and information warfare activities with a focus on understanding the intersections of disinformation and weapons of mass destruction (WMD). Prior to joining CSWMD, Gamberini was a Senior Policy Analyst with SAIC where she supported various WMD and arms control offices in the Department of Defense including the Defense Science Board and Headquarters Air Force.

Hello, I'm Sarah Jacobs Gamberini. I'm a Policy Fellow at the National Defense University Center for the study of Weapons of Mass Destruction. I'm speaking in my own capacity and not representing the views of the National Defense University, DoD or the U.S. government. Today I'll talk a little bit about quantum sensing's potential impacts on strategic deterrence and modern warfare and its implications for WMD.

Quantum technology is an area of scientific inquiry that receives a lot of hype, public interest, and media reporting. Because of its complexities and even spooky nature that defies even many scientific minds, many media and public policy discussions tend to lump quantum technologies together and talk broadly about "quantum". When we think of emerging technologies related to WMD, we often think about the implications of synthetic biology, artificial intelligence, machine learning, drones, or hypersonics. Quantum is usually put to the side, partly because it's extremely challenging to communicate to non-physics audience and partly because the timelines associated with potential availability are longer than some of the more present technologies that are not really emerging technologies, but are here today. But also because quantum is too broad of a concept to tackle without first breaking it down into the fields of quantum computing, quantum communications and quantum sensing. Much attention is showered on quantum computing and communication advances to transform commercial life and military operations. Yet the specific area of quantum sensing has important implications for deterrence and weapons of mass destruction. Quantum sensing has certain applications to the military that require extra diligence, investment and imagination. It merits additional discussion in the CWMD community.

So what is a quantum sensor? Like other sensors, it measures physical phenomena like magnetic fields or acceleration, but quantum mechanics allows sensors to measure with

higher sensitivity. They can have better long-term stability or smaller sensor size than other alternatives.

There's a wide range of these sensors from traditional atomic clocks, accelerometers, magnetometers, electrometers, gravimeters, and gravity gradiometers. And they can measure a range of things like frequency, acceleration, rotation rates, electric and magnetic fields, or temperature with high accuracy. Nearly anything that uses a sensor may be a candidate for a quantum sensor. But it's not a monolithic field and tech readiness levels vary greatly. On the one hand, technologies related to quantum sensing, including atomic clocks have been around for decades and underlie things like GPS and position, navigation and timing (PNT) technologies. On the other hand, there are quantum sensors in the lab that if employed in the field could disrupt some of our long-held thoughts on strategic stability and modern warfare.

Like many tech races, the first mover can exploit technological advantages on and off the battlefield. Let's take China. Quantum is an area China is investing heavily and during a period of great power competition, if the U.S. military fails to stay ahead in the race to field and integrate new or improved quantum sensors, there could be technological asymmetries for the United States. China's researchers are claiming they have a next generation quantum radar system that can detect stealth bombers and track ballistic missiles. There's been a lot of media hype about China developing a quantum radar, which if developed would be powerfully disruptive. However, the technology is not mature. Most agree that with today's quantum technology, quantum radars, like the one claimed by China are unlikely. There have been successes in lab settings, but this capability is a very long way off, if at all. And there are even questions whether they would provide any improved capability over other radars, but we still need to consider the real or perceived risks of falling behind China in an operational quantum radar race. From a deterrence perspective, the ability for China to field a fully functioning quantum radar system capable of detecting U.S. stealth aircraft would be disruptive to strategic stability in the region and undermine the survivability of America's stealth capabilities.

But we have to be incredibly careful in considering what Chinese researchers are claiming with a healthy dose of skepticism that allows us to confirm their claims. This type of quantum advancement could one day help China detect submarines. If this happened, it would place U.S. undersea deterrence at operational risk, including degrading the survivable leg of the U.S. nuclear triad. Since deterrence is based on perception, increased vulnerability due to degradation of stealth may reduce confidence in our ability to deliver an assured second strike nuclear response in the event of a nuclear crisis. This action would thereby undermine their credibility as a deterrent and erode their utility as a tool for allied assurance and extended deterrence.

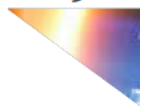
While understanding the threat of an adversary with this capability, it's also important to imagine the benefits of acquiring this technology ourselves. Submarines could use

quantum inertial navigation and help map and detect undersea ridges or canyons, and detect mines without relying on sonar, which can be detected by adversaries. There are risks and opportunities to any of these applications.

Now, not all quantum is decades away. As I mentioned before, the technology that underlies GPS is based on quantum in the form of atomic clocks. GPS is crucial for navigation, but it can be jammed or spoofed. Taking it to the next level and using quantum clocks might allow for orders of magnitude better precision. Quantum clocks are so accurate in fact that they would not gain or lose a second in close to 4 billion years. If quantum sensors can provide new PNT functionality, it could enable operations in previously denied or contested theaters like underwater or underground or provide more precision navigation in jammed or denied environments. And from where I sit at the WMD Center, one can imagine how these capabilities, once achieved, could advance military capabilities to target, track and locate WMD, including mobile missile tracking and targeting, hazardous material detection, and the entire spectrum of disrupting an adversary's ability to obtain and use a WMD. With the right imagination and advancements, the field of quantum sensing may be leveraged for innovative solutions to countering some WMD challenges.

Now, these advances could prove destabilizing if the United States and its competitors do not possess the same capability; but on the other hand, quantum sensing applications may offer the potential for increased strategic stability through reinforcement of crisis stability architectures such as arms control treaties and agreements. Detecting nuclear materials from afar using quantum sensors could offer a potentially improved range of compliance verification measures needed for accurate standoff, nuclear treaty compliance and verification activities. There are still some extremely hard and complex engineering and physics problems for quantum sensing's promise to come to fruition. This includes the challenge of miniaturization. Something might show promise in the lab, but transforming it into something that is compact, rugged, and autonomous requires funding and time. Another impediment to getting sensors out of the lab is the fragility of quantum system. Tiny movements, changes in temperature, or other environmental factors can disrupt the system, which is a challenge when we're talking about putting them in the field. But, if these engineering and physics challenges are overcome, quantum sensors could one day improve precision and accuracy of missile capabilities for us - or our adversaries like China who are already focused on improving their kinetic strike capabilities. So, there's both promise and peril in the future of quantum sensing applications, determining the technology's disruptive potential must factor in a number of things: Does the quantum sensor provide a better sensing capability than existing fielded systems or deliver the same capability at a far lower overall cost? Do we have the needed enabling technologies required to move these sensors from lab to field use? So, it's important to balance the cost and the gains

To conclude, for the U.S. military losing the race to field game changing quantum sensing



applications could lead to technology asymmetries. While quantum sensing technologies offer opportunities to transform modern warfare and certainly make the case for greater attention - they also present challenges and risks and face extremely hard and complex engineering and physics problems. We can't let that limit our imagination of what these technologies could do, because the fact is our adversaries are investing and researching. And if they overcome some of the engineering hurdles and are first to deploy some of these technologies, it will potentially destabilize both deterrence architectures and approaches to warfighting.

PROFESSOR GENEVIEVE BELL

Distinguished Professor Genevieve Bell is a renowned anthropologist, technologist, and futurist. Genevieve has a PhD in cultural anthropology from Stanford University and has worked across industry, academia and government. She is best known for her work at the intersection of cultural practice and technology development. She is currently the Director of the School of Cybernetics and Florence Violet McKenzie Chair at the Australian National University (ANU), and a Vice President and Senior Fellow in Intel Labs at Intel Corporation.

Hi, my name's Genevieve Bell. And I'm coming to you from Canberra, Australia. It's always a real privilege to get to participate in exercises like this. And I'm really sorry I don't get to be there in person. So, I'm doing the next best thing. I'm sending you some small thoughts that I hope are going to be really helpful and yes, I am sending them via PowerPoint. But before I get going, I want to begin by acknowledging the Traditional Owners of the land from which I'm speaking and pay my respects to elders past and present. I'm on Ngunnawal land here in Canberra, Australia - land that was always sacred and has never been ceded. I also know that this is going to be heard in lots of places, and I want to pay my respects to the Elders and Traditional Owners of those places too. For me, it's really important to think about where we start these conversations and where are the places that we anchor ourselves. And for me, I'm lucky enough to be in a place that has been continuously occupied for more than 60,000 years. And whenever I talk about the future, as I plan to do today, I get to do so in a place where people have been talking about, building and curating the future for well, as long as it ever was, and that is both an extraordinary privilege and a huge responsibility.

So where would you start in talking about the future? Well, there's lots of places, but for me, I always like to start with William Gibson. Gibson is a science fiction author and a writer, and has given us incredible works like *Neuromancer* and, of course, the term cyberspace. But back in 2003, he was being interviewed by a journalist from the *Economist* magazine. And the journalist asked him, you know, basically what's the future going to be.

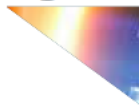
And I reckon that journalist was secretly hoping to get some great explanation about

technologies and blinky lights and shiny things. And Gibson said something that I think is extraordinarily provocative and really instructive when we want to orient ourselves to the future. He said: "the future's already here, it's just unevenly distributed". Like I said, an extraordinary provocation because it suggests if we're paying enough attention and we can find traces of the future already in the present of our lives, that if we look really closely, we can see glimpses of what's to come. People usually use Gibson to talk about technology. After all, most new technologies have realistically been years, if not decades in the making. AI was first defined in 1956, the internet in 1968 and so on. But if Gibson's injunction could also include how people behave and engage, I have to wonder where that might lead us and what traces of many futures we could find in this present.

And I'm thinking about this present. So acutely particularly. So I'm coming to you at this point from February 2022 in the future that is Australia. And I know here it's really tempting and hugely desirable to think that the pandemic's just been a momentary blip and that somehow we'll manage it and things will revert, or return, or resettle into some pattern we recognize. Of course, another way to think about all of this is that the pandemic's been an accelerant or an amplification of things that were already happening. It put tension on the system – well, put tension on lots of systems. And all the behaviors and practices that have emerged around the pandemic might then be worthy of examination rather than thinking of them as an aberration or something that we hope we can get past - maybe we should think about them as glimpses of a future that's already here.

And if you were to do that, I think there's five threads that emerge out of the pandemic that might be really useful for how would think critically about the ways that individuals and groups function and engage and in doing help frame the questions I know you're all grappling with in a slightly new and different way. So, let's go.

One of the pieces of the future that you can see in the present is the relationship between the local and the global. My suspicion is for a couple of decades, we've thought of that as oppositional, we've talked about globalization or localization. I think one of the things the pandemic has made really clear is that these things operate together and apart, and that neither of them are coherent, nor is the relationship between them. We've seen the rise of new global actors who have been gaining enormous authority. Whether that's the World Health Organization, doctors, geneticists, we have seen a capacity to think about giving people authority in ways that's simply not been the case before. We've also seen the willingness of nation states, in particular, to shut their borders, to stop their citizens from moving around and to do so under the umbrella of public health but at a scale that I think we would not have anticipated even five or 10 years ago. We've also seen the importance of local communities rising up and managing themselves against that backdrop. And we have seen the interconnection between all of those systems made hyper-visible, whether it's about plane routes, the way viruses travel, or the way supply chains do and don't function. And if you are wanting to think about how groups' behavior might be influenced in the future, you have to be thinking about local and global tensions between them and



the new actors that are being thrown up.

Building on that notion of the local and the global, one of the other things that has been, I suspect, accelerated during the pandemic is the disconnection or the uncoupling of the relationship between power and authority. How is authority understood or adhered to? Who gets to have power? And where is it? Those have always been open questions, but over the last two years, the complexities of all of that is infinitely more on display. Which means that who gets to be the voice of authority, how that authority is manifested, and who is listening is nowhere near as stable or as seamless as it seems. I also suspect we have continued to see the fragmentation of the relationship between capitalism and democracy. And I know that sounds heavy, but imagine that capitalism no longer needs democracy to flourish and democracy doesn't quite know what to do about that. And now imagine you are a group thinking about how you want to behave, where you derive power from and how you might respond to authority or authority figures and you start to imagine that some of the pieces of the puzzle are infinitely more complex. Oh yeah, and layer on top of that, that we have seen the continued rise (and I would say acceleration) of moral authority as opposed to the kind that comes through an obvious institution. I'm thinking here of the "black lives matter" movement, but also the "me too" movement and the various ways in which those have been contested and labeled and what it might mean to think about the idea of counter-authoritarian or counter-authority moves and organizations who see themselves as having power and authority but those are not formally structured, but they are globally or nationally recognized.

One way to think about the rise of moral authority and the notions of moral authority sits on another piece of the future that I think has been in sharp display recently, which has to do with the ways in which narratives and stories are proliferating and the need for coherence is diminishing. It is absolutely the case that a story and storytelling forms have gotten shorter – so, I'm thinking here of TikTok or Twitter - the need for coherence has given way to notions of image and action and movement. So, we're starting to see symbolic regimes untethered from the ways that they have meaning and a host of new narratives or perhaps old narratives resurrected around danger and fear, especially when it comes from ideas of other, whether the other is a virus or people who don't look like us or places that don't sound and feel like us. It's a mobilization of a very particular set of stories, but think here about the rise of new channels, for information distribution, new kinds of stories, and increasingly fragmented pieces of the story that no longer need to ladder up to a narrative. And it makes it even easier to imagine how you might bring an entire group of people along with you if you have a set of images, a short set of narratives that have punch or power to them, but not necessarily coherence. It also means how you resist or dismantle or unpack the power of those narratives is even harder than it once was.

Of course, part of what's going on here is that we're also seeing a change in our notions about time and the way time unfolds. Time is another thing that the pandemic has

disrupted and where the future is kind of just peeking through - it is that we've shifted our sense of time and timeliness and our notions about how long things could or should take and who gets to determine how long something takes and what are the rhythm of things. Although, I guess one of the other ways of thinking about the consequences of all of this, where I suspect it is the future on display - is that it turns out you don't have to impose very much uncertainty on the system in terms of a timeframe or in terms of time before you fundamentally destabilize the whole. So, part of where the future might be sitting on display now has to do with the relationship between time and uncertainty. How much do you need to undermine before the whole becomes even more fragile?

And last, but by no means least, I think the final piece of the future I have seen in the pandemic is the rise of the non-human. We spent a lot of time before the pandemic talking about what it meant to be human. We have spent a surprising amount of time during the pandemic, thinking about non-human actors in relationship to the human. So not understanding who humans are, but starting to look at the rest of the world around us, whether that's about the behavior of viruses and ecosystems and the ecology, whether it is also about the behavior of animals and even gods and forces unseen to us. I think one of the unexpected tantalizing glimpses of the future I have seen of late has to do with what happens when we stop thinking that it's all about the human and start imagining it's about other things. And how those other things get mobilized for me, feels like an unexpected source of both power and possibly confusion.

So that was a lot of words and a really quick drive through about the pieces of the future I'm already seeing now. And I know you're sitting there thinking what am I going to do with all of that. The reality is that human beings change slowly, but catalyzing events like the pandemic may accelerate a whole set of trends that were a long time in the making, whether it's about how we think about power, how we think about the nation state, how we think about communication, time, and even who we are and what our role is in society and the world. All of those things are in movement and all of those things will shape groups and the ways in which they think about themselves, their landscape, their enemies, and how they might want to prosecute their case.

PETER WARREN SINGER

Peter Warren Singer is Strategist at New America, a Professor of Practice at Arizona State University, and Founder & Managing Partner at Useful Fiction LLC.

A New York Times Bestselling author, described in the Wall Street Journal as "the premier futurist in the national-security environment" and "all-around smart guy" in the Washington Post, he has been named by the Smithsonian as one of the nation's 100 leading innovators, by Defense News as one of the 100 most influential people in defense issues, by Foreign Policy to their Top 100 Global Thinkers List, and as an official "Mad Scientist" for the

U.S. Army's Training and Doctrine Command. No author, living or dead, has more books on the professional US military reading lists. His non-fiction books include Corporate Warriors: The Rise of the Privatized Military Industry, Children at War, Wired for War: The Robotics Revolution and Conflict in the 21st Century; Cybersecurity and Cyberwar: What Everyone Needs to Know and most recently LikeWar, which explores how social media has changed war and politics. It was named an Amazon and Foreign Affairs book of the year and reviewed by Booklist as "LikeWar should be required reading for everyone living in a democracy and all who aspire to." He is also the co-author of a new type of novel, using the format of a technothriller to communicate nonfiction research. Ghost Fleet: A Novel of the Next World War was both a top summer read and led to briefings everywhere from the White House to the Pentagon. His latest is Burn-In: A Novel of the Real Robotic Revolution. It has been described by the creator of Lost and Watchmen as "A visionary new form of storytelling—a rollercoaster ride of science fiction blended with science fact," and by the head of Army Cyber Command as "I loved Burn-In so much that I've already read it twice."

I'm someone who wrestles with the future. And there's a challenge in that. There's a belief that it is something that is impossible to predict. Indeed, a senior U.S. defense leader described how trying to project the future was like "driving in the dark with your headlights off." As in that's something you ought not to do.

There are two problems with that. The first is that we don't have a choice. Whatever role you play, whether it is in training, acquisitions, strategy, budgets, etc. you have to make assumptions about and decisions about the future. You have to drive in the dark.

The second is that there's an interesting pattern that happens when we look not towards the future, but rather towards the past. When we've gotten the future incorrect, whether on major intelligence failures like 9-11 or Pearl Harbor to doctrine or acquisition program failures, consistently, the failure is not from a so-called "Black Swan." It is not some kind of unimaginable that no one could predict. Rather it is repeatedly what is thought of as a "gray rhino". It is a trend, a topic that was fairly obvious. But, it was just uncomfortable to look at, to admit that it was in the room with us.

So, when it comes to the topic that I've been asked to speak to you about, technology and security issues, what is it that lies in right in front of us, but is hard to wrestle with its full importance?

I think the trends are fairly clear and obvious. It's the leap of game changing technologies that are playing out over the next decade plus in the realm of artificial intelligence. We are seeing breakthroughs in a technology that is something that we've waited for and talked about for literally millennia. You can find discussions of artificial intelligence and everything from ancient Greek mythology to old Judaic texts. Maybe you're a science fiction person. Well, for over a century, we've been talking about this moment, when AI becomes real.

To be clear, it is not just the software side of AI. It's also about the hardware side of robotics and its advancement playing out in all sorts of shapes, forms, roles, and users. But again, don't just think about this as a technology that might be out there in the field and playing out in terms of security. It's also how it affects the broader economy and society writ large. For example, Oxford University did a study of 702 different occupational specialties and found that roughly 47% of them are at risk for complete replacement, reduction, or drastic redefinition over the course of our lifetime.

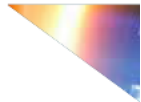
Importantly, each of these areas have their military parallels. Again, so the real looming change with robotics is not the so-called lethal autonomous weapons system, killer robots, or nuclear weapons being controlled by AI that get so much discussion. It's about how AI covers the entire spectrum of application, in everything from decision helping to military medicine, to logistics you name it.

The shift is also another kind of change, not just in terms of the software and the hardware, but what binds it together in terms of the network. We see this playing out in a couple of key ways. One is in the weaponization of social media, where you've seen the impact affect everything from politics to public health to battlefield behavior to even being wrapped up in the story of mass killings going after hundreds of thousands of people. This area is gonna get even more challenging in the coming years because of one of those prior topics, artificial intelligence. The line between what is real and what it is not is already very tough to figure out now. It will be even more so as we blend in greater levels of AI – what is popularly known as “deep fakes.”

But there's a second key change in terms of the network. It's the shift of the internet from being about merely communication, which was game changing enough, to the concept of the internet of things. It's an idea that originates in 1999 and is becoming real now, where we are using the network to control the operations of everything from smart cars, smart power grids, thermostats to the individual parts of systems. Now, that will open up huge possibilities, of over \$11 trillion in value, but it'll also open up new risks. It doesn't just drastically grow the attack surface of what you might go after. It also changes the kind of effect that you might have with a digital attack, where you're not stealing information or spreading information, even if it's false. In this case, you are causing kinetic change in the world, physical damage.

We're also seeing a whole change in terms of the very approach of computing itself. When you think about quantum technology, such as a project that we are doing with NATO ACT, we will see the ripple effect in forms of computing, communication, encryption changes to sensors.

My point in this quick tour is that if you pull back and think about it, we have a massive rethink of not just technology and its possibilities and perils, but also what it means for the battlefield itself. Now that is very bold to say, but again, look back in history. Why should we think these changes in everything from AI to robotics to quantum are somehow



gonna be less in their effect than say the machine gun in 1914 or the tank and the airplane in 1939. And, in fact, shouldn't they be something more, because we're talking about a technology that unlike ever before is always improving, ever more intelligent, ever more autonomous?

So what can we do about it? Well, I would argue there's a series of measures that we need to undertake. One: Education and awareness is now a core task of leadership. For example, in the case of AI, 91% of leaders say AI is the most important game changing technology that's out there. 17% - though - say they understand AI, how it works, what are its ramifications and its dilemmas. That is a massive delta between what you think is going to be important and how well you understand it. And it's not just specific to AI; it's any of these new areas. It's not just about looking at yourself, it's looking at your organization and asking, "Not just what is important, but how well do we understand it?"

Second: Every aspect of this is not just a story of technology. It's a story of people. And so, how are we looking at how we handle talent management? In all the human questions, everything from recruiting to assessment, are we making changes that are equivalent to these other changes that are going on out there? And, if not, why would we expect the human side to keep pace?

Third: The key issue of trust in all of this. But it's the dual meaning of trust. You can think of trust as a kind of emotional state, as in "I trust you." But it also has a definition in terms of how engineers might think of it. Does it behave in an expected manner? Does it match the way that we understand the world? So think about it this way. You can "trust" someone, but you can also "trust" that someone is a liar and that they're always going to lie to you. And so with that expectation that they will always lie, you can operate effectively in the world, even if you don't trust them. And so these two meanings of trust are the key to not just integrating the technology and using it to its full effect. But also these two meanings of trust are how any adversary is going to go after us.

Fourth: another part of this in terms of these dual issues of trust, but also a larger sweep of change - is how it will affect what we're thinking of as multi domain operations and the task of multi domain integration. Essentially, this is how the technology is going to affect not just overall security, but battlefield behavior. And when you get inside this, it also cuts to the heart of the new concepts and doctrines that we need out there.

What is our vision of the technology and our relationship with it in terms of everything from trust to the uses that we make of it?

For, example, is it a tool that we are using? Or is that technology not just merely a tool, but it is something equivalent to a teammate, a partner, a part of the organization, a wingman? Or, is it beyond the equivalent of a tool or a partner, but an autonomous agent that we delegate out there? And not just that we delegate it out there in a single form, but also maybe we delegate it out there in terms of a massive number, a swarm that has agency

of its own? How we answer these visions, is again, key to the future, whether we're talking about the future of cyber war, air warfare, etc. and also how they come together.

Fifth: But it also means that we need to undertake another kind of change. We need to change how we visualize and train for the future. Too much of how we approach it right now is validation: validating existing concepts, existing technologies. Or is is validating our existing relationships, the kind of exercises that we love to do. "We're allies, let's go out there together and show how much we like each other and can work together" That definitely has value, don't get me wrong. But we also need to do more of the kind of exercises that we saw back in the 1920s and 1930s, whether you're thinking of the British Experimental Mechanized Force or the American Army's Louisiana Maneuvers. The goal was not just to figure out the difference between horses and mechanization, but how is this technology best used in everything from the doctrine to the tactics. But the big lesson from that period is again, it's about the people. It is about figuring out who's thriving in these exercises with what kind of mentality and training? And then the most important lesson is not just learning the lesson, but how do you actually implement them after the exercise? Because sometimes the insights get implemented and a lot of times they don't.

As part of this, you should also be seeking out lessons in terms of not just what works, but what doesn't - before you actually commit. This image is an example from U.S. Navy exercises in the 1920s, where they wanted to learn about the new concept of an aircraft carrier. There were two different approaches to it that you can see here. The USS Patoka on the left was the aircraft carrier for blimps. And the USS Langley on the right was the aircraft carrier for planes. Now compare that approach, where they actually went out there and wrestled with the varied approaches, to how we would do it today, where we already commit to not just the concept, but entire ship classes before we've actually figured out what works or not. It is better to learn during experiment then later on in a war.

Seventh: You also wanna learn from other people's wars. So again, go back in history and the example of how the Blitzkrieg seemingly surprised its foes. And yet, it was all tested out in the open in the Spanish Civil War.

So, what about those other nations' wars out there today? What can we learn from the. Everything from what's happening in Libya to Ukraine, to, as you see on the right, the war between Azerbaijan and Armenia. Through very skillful use of bringing together electronics, cyber, unmanned warfare, the kinetic and the digital side, the Azeris were able to take out, at least according to open source intelligence, 46% of Armenian armored vehicles and 93% of their artillery missile systems in just a matter of weeks. That kind of change is important, not just for that conflict, but what it means for all the other future conflicts out there.

Eighth: We also need to change the way that we visualize and communicate. There are more effective manners than producing white papers that people don't wanna read, or they don't digest the insights from it. We've been using a practice that we call "useful

fiction.” It brings together non-fiction analysis and research with the oldest communication technology of all – narrative. You can think of useful fiction in a different way as being akin to a morning smoothie. Science fiction and techno thrillers are like a milkshake; they're entertaining, they're tasty, they're fun. At the other end of the spectrum, you've got the vitamins, kale, something that's good for you. That's that research, that's that strategy paper. Useful fiction is like a morning smoothie. It takes the kale, the vitamins of the insight, but wraps it within a tasty package.

An example of the potential of this is a project we did with the Australian military that you see here. They had a 21 page report on defense education enterprise reform to deal with some of these new issues that we've been talking about. It's a great report, but it wasn't striking with a desired effect. So we worked with them and took its three key themes and 37 key insights of that report and turned it into a narrative and a piece of art called “An Eye for a Storm.” It took the key ideas they wanted to share, but blended them into a story that follows a young officer from war college to an exciting mission, an embassy evacuation in the wake of a tsunami. In terms of the impact of it, it's been read by over 14,000 readers, all the way up to the head of the entire Australian military and six current or recently retired U.S. four stars. By bringing in narrative, we were able to reach an audience that a typical white paper would not be able to. And, if you can do this kind of approach on a topic as dry as defense education enterprise reform, you can do it on any topic,.

Tenth: Finally, we need to kill our sacred cows. What is the equivalent to the battleship in 1941 or the horse cavalry in the 1930s? What is that technology that is not ready for the future war, probably not ready for the present of war?

But, again, it is not just about the technology. What are those organizational structures that were developed for the past, but aren't appropriate to the present and future? Hint: you can identify sacred cows by not just what's not ready, but what is it hard for us to talk about out loud?

And, so with that, I know I've thrown a lot at you in a limited amount of time. So, I would leave you with just one key takeaway: Think of all of the change that's going on out there around us, whether it's technology, security, politics, society... Given all that change, any nations, organizations, or individuals that look at that change and decide to stay still? They will be choosing to lose the future through their inaction. And I hope none of us do that. Thank you.

COLONEL BETH L. MAKROS

Colonel Beth L. Makros is the Permanent Professor and Chief Learning Officer for the Commandant of Cadets at the US Air Force Academy. In this role, she is responsible for overseeing and integrating all military education and training for over 4,000 cadets. A

command pilot with more than 2,000 hours, she has served as an Air Operations Center Commander, Squadron Commander, Deputy Mission Support and Operations Group Commander, Director of Operations, and Instructor and Evaluator pilot in both the B-2 and T-38.

Greetings for the United States Air Force Academy. My name is Colonel Beth Makros. I'm a professor of military and strategic studies here at USAFA. My background is primarily from weapons of mass destruction within the nuclear operations enterprise. I have been a planner at STRATCOM in the J5 writing the O-plans for many of our nuclear war plans. I have served as the commander of the air operation center to STRATCOM's JFAC, and then I have over a decade of flying B2, nuclear capable bombers. So, my approach to this conversation of weapons of mass destruction will largely be how does it impact our nuclear operations.

Before we get into more specific emerging and disruptive technologies, I'd like you to consider two things and keep in the back of your mind two considerations. The first one is to realize that nuclear weapons are largely in existence for the purpose of deterrence. And when we talk about deterrence, we're really talking about the efforts to shape the thinking of an adversary or more specifically the decision calculus of the decision maker from that adversary. So it's getting into the cognitive processes for each decision maker or makers for a given adversary and understanding what might cause them to make certain risk calculations or decisions. So you want to consider, for each of these technologies, sort of does this technology change, or how does this technology change the decision maker's calculus as far as what he or she or the group would likely do? And does it cause an inadvertent escalation so that they might be more incentivized to use their weapons of mass destruction? This second thing to realize is that deterrence and strategic stability largely exist because of an assured retaliatory strike or often you'll hear it called second strike capability. No one country has the ability to completely eliminate the weapons of mass destruction for another country, the way it stands. And that keeps us in somewhat of a stable atmosphere. So, when considering new emerging and disruptive technologies, how might that impact the strategic stability that already exists? Might it impact the retaliatory strike? Might it impact the assured use of a weapon? So again, if a country is concerned that you might be negating my retaliatory strike capability or my ability to employ my weapons, might there be a first user or first mover impetus to use those weapons before they lose those weapons. So those are two things to consider as we talk through each of these technologies.

So, the first technology I'd like you to consider is artificial intelligence and autonomous weapons. So, what is in the realm of possible here? Well, autonomous weapons could be used to launch and loiter for long periods of time looking for certain patterns of life or recognition of weapons systems or behaviors or be programmed to use when X event happens. So currently, as we think about the stability of weapons of mass destruction, there's this gap of time when an event happens before a decision maker makes a decision

whether or not to use a weapon of mass destruction or respond to the use of a weapon of mass destruction. That's the time where they're using human cognitive processes to sort of do risk analysis and decision making. But if we introduce this idea that there's autonomous weapons out there just loitering for an event to happen, and they are programmed to strike immediately then does that potentially negate that humanness or the human in the loop for making a decision when we're thinking about weapons of mass destruction? What if we give up that decision making to autonomous weapons or AI, how might that impact our strategic stability? If I think you might be negating my ability to use my weapons of mass destruction, does that shorten the timeline between detection of an event and the execution of event in using WMD? And how does that change the decision making on that cognitive processing for a decision maker? Does it take it out of their hands totally?

The second technology I would consider that I think has massive implications for weapons of mass destruction is quantum computing and the use of quantum physics and sensing. So right now, when we talk about quantum computing, what's in the realm of possible for the near future? It's computing at speeds that improve secure communications and encryption and navigation (precision, navigation, and timing). All of those things can massively change the way in which we execute our weapons of mass destruction, because it allows us to be potentially more precise or the ability for us to have such incredible encryption that no one would be able to get inside that decision making, but the same is true for our adversaries. They might be able to break our encryption and see what is happening long before we could ever make an execution.

The second thing is to think about detection. So again, I mentioned, I flew stealth bombers. The stealth world relies heavily upon the ability to evade or at least be under some type of radar cross section threshold so that we can maintain a stealth for penetrating into adversaries areas that we would like to potentially use the weapons on. Well, in quantum, that ability to sense might override what we know to be the stealth technology that we rely upon. So what if in the quantum physics they're able to use the quantum particles in order to detect stealth. Does that negate stealth altogether? What does that mean? Particularly for our submarines, that we highly rely upon for that second strike capability.

Okay. The fourth technology is the use, uh, or I'm sorry. The third technology is the use of hypersonic weapons. So hypersonic weapons, anything that goes up above five times the speed of sound or five mach. So, but these new hypersonic weapons that we're seeing, whether we're talking about glide vehicles or scram jet type of technologies. They really are able to maneuver in a way that is quite different than ballistic missiles. So, we can see ballistic missiles. We can see the launch, we can see the threat band as we start to see that it's trajectory. And then as we get dual phenomenology and we see it on radar, we can create an ellipse knowing where that ballistic missile is going - in sufficient time that we can move our aircraft or potentially launch our intercontinental ballistic missiles so that they're no longer under threat. But with hypersonics, those are maneuverable. And while

not traveling at the speeds that the ballistic missiles are - still traveling at fast speeds. So what does that mean? One that they can potentially negate our ability to launch, because we don't know where that weapon is going to - so they can negate our assured strike. But the second one is what if it can potentially take out your command and control facilities or your command and control capabilities. So you no longer have the assured strike capability. You no longer can talk to your weapons. You no longer know where a weapon is heading to and what the impact of that weapon might be.

And the final technology is just the increased use of space and cyber on our weapon of mass destruction and on the systems that enable our assured, secure weapons, particularly in the nuclear enterprise. So the nuclear use is highly, highly dependent on the national command and control and communications (NC3 capabilities). It is a system that is secure and persistent. It is the ability to detect, decide and execute an order from the president to use weapons. NC3 resides or requires a large number of space assets to do that. So that ability to take out space assets for the U.S. and impact our national command and control and communication system is one that would be very concerning for the U.S.

Okay. I hope that is helpful in getting some thoughts on different technologies. Again, I think artificial intelligence, autonomous weapons, quantum computing and sensing, hypersonic weapons, and the use of space and cyber to attack our command and control authority are things that we are greatly concerned about for our ability to use weapons of mass destruction in the future. I wish you the very best wish I could be there with you all in this endeavor. Take care.

ANDREW HESSEL

Andrew Hessel is a scientist, communicator, and investor exploring the future of biology and biotechnology. He is the co-founder and chairman of the Center of Excellence for Engineering Biology and the Genome Project-write, the international scientific effort to design and build large genomes, including the human genome. He co-founded Humane Genomics, a developer of precision artificial viruses that target cancer. Andrew is a former distinguished research scientist at Autodesk Life Sciences. His new book, The Genesis Machine: Our Quest to Rewrite Life in the Age of Synthetic Biology, co-authored with Amy Webb, was released in February 2022.

I'll kick this off. Thank you. So again, when it comes to weapons of mass destruction and kind of the current ranking of first nuclear, second cyber and third chemical, I completely acknowledge that these are important areas. These tend to be areas that are number one outside of my domain of experience. When it comes to nuclear, I'll just put that whole thing in a box and move it somewhere else, because I'm not a nuclear scientist.

Cyber I think is absolutely essential today because it is one of the emerging domains of warfare that is within reach of just about any participant, from a single individual to a nation state. We're seeing it play out today in the real world, in Ukraine, we've seen, certainly attacks in the U.S. and other places. Very important and will no doubt be enhanced by the continuing advancement of machine learning, AI and other technologies. But again, not my complete area of experience. So I'll put that in a box and just say it is important.

Chemical is not something I particularly worry about because that requires significant manufacturing capability to affect large populations. Chemical attacks can certainly happen on a smaller scale. Chemical accidents can occur and affect local populations, but for a mass destruction event, at a global level, I don't worry too much about chemical.

The area that I have been speaking about and highly concerned about is actually biochemical warfare, or what some people might think of as biological warfare. I look at biological systems as being completely programmable as genetic technologies have continued to advance. And what I mean there is the ability to sequence animals, plants, people, et cetera. That technology has advanced at a remarkable rate over the last 20 years. We have seen this with the human genome project. The first genome costing billions and literally producing a single consensus genome. To today being able to get a clinical grade genome in hours for a few hundred dollars. So that is, the ability to read genomes has far outpaced our ability to even fully comprehend the risk. The ability to analyze genetic data is moving at a remarkable rate again, assisted by cyber technologies, machine learning and AI. But it's the ability to write genetic programs using DNA synthesizers that is also moving at a super exponential rate and opens the ability of programming cellular and cell-free biological systems, viruses, and virus-like particles to essentially anyone that is willing to put in a bit of time, effort and investment, like cyber, from a single individual to a nation state. I look at that as being the biggest risk factor as a weapon of mass destruction today because these tools and technologies and capabilities are here now.

My previous company designed and built viruses from scratch targeting cancer cells. I was astounded by the pace of synthetic biology and the genetic engineering technologies to do that. In the last few years, it has become trivial to design and build a virus really for a few thousand dollars and a few weeks of work. And this opens the possibility of making virus like COVID but also viruses that are much more infectious and potentially much more deadly or pernicious. For example, weaponizing some sort of neurodegenerative disease. This is, in my opinion, the most significant near-term risk for a weapon of mass destruction, because it could be achieved by even a single individual. It is not prohibitive in terms of cost and because it is a self-manufacturing, self-replicating, and really self-spreading vector. I think the asymmetry between production and defense is gigantic today.

COVID taught us that we simply did not have the right detection systems and the right

defenses for self-replicating particles (like a virus or a virus like particle) and I think those gaps still exist today, and I think they will continue to exist without global cooperation and massive investment in detection and remediation technologies. I point out that a lot of my thinking is very similar to the author and technologist, Rob Reid, who has spoken eloquently on the risks of viruses and virus-like particles and their potential abuse.

The only thing that scares me in bioengineering as a weapon of mass destruction is a virus or virus-like particle because these have very small genomes or genetic constructs when it comes to engineering. So, the technology already exists. They're not expensive to make, and you can make combinatorial libraries of these agents trivially. So, making large combinatorial libraries, running them through filters of infectivity and pathogenicity will quickly allow the production of something that is truly scary, even a potential civilization stopper. So, it's only viruses and virus-like particles that keep me up at night. The idea of a scientist doing an experiment that accidentally produces one of these particles, follows them out of the lab and potentially spreads around the world is a real and valid concern. We may not detect something like that till well after it's spreading and starting to cause a problem. As we're aware, some people believe that is what actually happened with COVID.

I am particularly concerned that we don't have proper tracking and accounting of virus engineering and virus-like particle engineering in labs around the world. It is largely research and development directed by individuals and companies with very little accountability and tracking, except for a small number of select agents. I think this is naive. There are billions of natural viruses. Humans are just one target, plants and animals are other targets. So, it is relatively straightforward to do this work. And again, it keeps me up at night because we're just so blind to the work that's being done, any viruses that are circulating naturally, any viruses that may be engineered and circulating. We also have so few therapies and responses for a virus infection. We know that we made history by producing COVID vaccines in nine months. That's, let's say, eight and a half months too long to respond to something urgent. We absolutely have to shorten the development path for countermeasures.

So between the lack of detection systems and the lack of speedy countermeasures, I think this is one of the largest risk factors and will remain a risk factor until we harden and bolster those systems. Which I believe is an absolute essential over the next 10 years.

U.S. GOVERNMENT EMPLOYEE

Today, I want to start as we have to start every one of these by saying these are my own opinions. These are not the opinions of the Department of Defense, the Air Force or the U.S. government.

Now for your question today: which is what is the future implications of emerging

destructive technology on WMD warfare? We've got a few trends that I think would be helpful for you to focus on. Among those clearly, from an air force perspective, is going to be exquisite technologies, right? So right at the top of that list are hypersonics. If you're not looking at hypersonics and the destructive capability of hypersonics, what can be done with them, who has them, who will have them and different timelines associated with those hypersonic productions at scale and what they look like in warfare, what that decision time means and the shrinking decision time means across the spectrum warfare. You've really got to take a real serious look at that.

From a general perspective, think of shrinking decision times when you're thinking about WMD. This isn't a, we don't have even the old, you know, hours or days or months, we were talking minutes, we're talking seconds in some cases, depending on what is occurring, right. And we know this from the cyber realm.

Okay. Uh, another thing that we're gonna hit for you guys, I think is probably gonna be pretty important here, clearly bio weapons. All right. So from CRISPR for gene editing the entire, you know, there's a lot of different ways these be made, not just by governments, but by non-state actors as well at a relatively easy level. Now the scale of these and what can be done, varies widely. But we want to, to think about here is: what are the effects? So what might they go after, besides what you normally think of, um, kind of a caveat to this is think a little bit about from a sustainment progress or a sustainment point of view, uh, life sustainment, what needs to happen in order for things to live for things to exist. If you wanna think about lethality, what needs to happen for life? And how might you target those key natural resource or key requirements. Think of Maslow's hierarchies of needs and what needs to happen for that to occur. So that's something to keep in the back of your mind when you're going through the process today.

Some other keys we wanted to hit for you today. We're talking clearly nuclear, you cannot think about the nuclear about WMDs and the nuclear arsenal. If we're not thinking about where that's going, who has it, scaling on nuclear, what that means, um, from small to large and everything in between. Um, and then within that, I think what's a key variable through all of WMDs is the idea of asymmetries of will or ethical asymmetric are part of that. So someone's willingness to use it. What might some nation states or non-state actors be willing to do that others may not. Where are those barriers and how are they changing and how are they shifting? How are those norms eroding or being eroded or being pushed back? What can be done differently - from treaty bodies, uh, and the way we're organized, um, you know, how effective are these actually being and how might they be in the future and what's being done to undermine them, uh, or to strengthen them. So that's something we might want to wanna probably give a little bit of time too.

Along with that, we'd be remiss if we didn't speak a little bit towards, uh, pushing the future forward on the technological front. Um, and in cyber, I think quantum is a game changer. Two big game changers on the tech front - one is energy and the ability to store

unconstrained energy, as that comes down the line, we're probably not looking out at 10 years for that, but cheaper, more effective, portable energy is one big thing to look at for move maneuver. Also, what that means for directed energy. So that's something you also wanna be thinking - kinetics, but if you aren't thinking the non-kinetic, you, you're not thinking warfare in the future. We really wanna make sure you're thinking about how cyber and WMDs and all the kinetics all work together, you know, as a series in warfare and what that means. Series or in parallel, depending on how you want to deploy them.

Another key point, uh, one to raise just a little bit, before we hit the five minute mark: is think about resiliency as well. At the end of it, we can think about stopping the WMDs, but we also need think about the after effects from any attack. If we can't stop it, how do we bounce back?

So two other quick points, one do not presume sanctuary anywhere at any time, right? That's what the war of the future may well look like now. Oftentimes we think of North America as its own safe block, right? The Homeland is secure. We can't think that way anymore. We need to think about a world that's interconnected in a way where all the different systems are linked. Within that, another key that I think you should think about as well as supply chains. And not just how we think about supply chains now: how they can slow information or slow material from flowing from one place to another and key resources from getting to what you need, but also think out how they can support what you need to get done. How do you make supply chains resilient? How do you make them get what you need on time, where you need it? How do you use them in a way that builds that belts and suspenders? That extra safety, that extra resiliency to get to where you need to go and help you protect all of your assets, wherever they are.

I think these are the key points that we wanted to hit for you guys going forward. We might have a few more, uh, as we go, but I think this is really what we wanted to get across at the moment. So without further ado, good luck today, have a fantastic Threatcasting experience. We really look forward to reading and seeing your report. Good luck.



APPENDIX III

A HISTORY OF THE NATION-STATE

A brief selection of historical events and case studies are provided below, which cover nearly four centuries of state and non-state power struggles. These anecdotes from 1618-2015, help illustrate the relative “newness” of the concept of nation-states and how it continues its evolution today in an era of modern competition.

1618. In 1618, the Thirty Years War began. This exclusively religious war savaged Europe. Conflict was vicious, pervasive, and crossed all borders and boundaries - as every side fought for religious universality and religious solidarity.

1648. In 1648, the Peace of Westphalia ended the Thirty Years War. The Peace of Westphalia was not a single treaty, but rather a collection of agreements. A devastated European continent ultimately agreed to disagree, establishing a basic order that we reference today. In Kissinger's words, "The Peace of Westphalia became a turning point in the history of nations because the elements it set in place were as uncomplicated as they were sweeping. The state, not the empire, dynasty, or religious confession, was affirmed as the building block of European order. The concept of state sovereignty was established."¹¹ This new order enshrined the principles of multiplicity and balance of power. Equilibrium became a primary goal of international relations. The inherent sovereignty and legitimacy of states formed a foundation for this order, which mostly held together for nearly two hundred years. The concept applied only in Europe, however. Colonies in Asia, Africa, and America were thought to have no such sovereignty, and Westphalia placed no limits on company-states. Colonialist exceptions eventually led to the system's collapse.

1757.

Case Study - English East India Company Wins the Battle of Buxar

Chartered in 1600, the English East India Company (EIC) came fully into its own in the 18th century, growing into a behemoth quasi-state that ruled huge portions of the world. One renowned historian argues that the Battle of Buxar was the critical moment of change

for the EIC. By defeating three Mughal armies at this battle, "the Company was left the dominant military force in north-east India.... The Company, which had started off as an enterprise dominated by privateers and former Caribbean pirates, had already transformed itself once into a relatively respectable international trading corporation, with a share price so reliable, its stock was regarded almost as a form of international currency. Now the Company was transformed a second time, not just as a vehicle of trade operating from a scattering of Indian coastal enclaves, but as the ruler of a rich and expansive territorial empire extending across South Asia."¹¹²

1792. In 1792, the French National Assembly proclaimed support for revolutions everywhere, undermining the Westphalian principle of sovereignty. This new crusade, secular and ideological, revived some of the sectarian fervor that had fueled the Thirty Years War. In the minds of revolutionary leaders, the principles of liberty and equality trumped earlier state legitimacy.

1815. The "revolutionary leader" model was called into question as the 1815 Congress of Vienna ended the Napoleonic Wars. European states scrambled to establish a new balance of power that placed the necessary constraints on French aggression. The resulting agreements merged a number of smaller central European states to better preserve the balance of power. The system, set out by the Congress of Vienna, had two main components: the Quadruple Alliance of Britain, Prussia, Austria, and Russia was to defend the territorial order, while the continental Holy Alliance of Prussia, Austria, and Russia focused on maintaining internal order in an effort to avoid excessive liberalism and revolution.¹¹³

1852.

Case Study - Pinkerton's National Detective Agency was Founded

Pinkertons were much more than private detectives—they were infiltrators, enforcers, fixers, even considered a "lynch mob for hire". "In an age of new market discipline and territorial expansion [1852-1937], Pinkertons served as a quasi-official extension of the state where the state had little other representation. As rapid industrialization triggered bloody labor conflict, the agency became, for all intents and purposes, capital's private army." The Pinkertons were a critical force in strike-breaking and terrorizing labor on behalf of late 19th century industry, leading one historian to argue that the agency "was a pivotal institution in the formation of American monopoly capitalism. Through the Pinkertons, American capitalism implemented and enforced new structures of order on industrial frontiers The state, at the federal and local level, not only refused to limit the scope and

¹¹¹ Kissinger, *World Order*, 26.

¹¹² Dalrymple, *The Anarchy: The East India Company, Corporate Violence, and the Pillage of an Empire*, 201.

¹¹³ Kissinger, *World Order*, 65.

power of the agency but also actively legitimized the Pinkertons by hiring and deputizing the agents. The state both exercised its power and contracted out its authority through its use of the agency."¹¹⁴

1871. In 1871, the end of the Franco-Prussian War unified Germany and stabilized the previously fluid balance of powers. When Otto von Bismarck united Germany, his concept of world order centered on nationalism and power rather than the balancing principles of the Holy Alliance. Germany rapidly defeated France in the Franco-Prussian war, annexing Alsace-Lorraine. Bismarck proclaimed the German Empire from the Hall of Mirrors at Versailles. No longer a fluid balance of powers, Europe became a web of fixed alliances and began a pattern of confrontation and industrial military armament.

1918. The 1918 Treaty of Versailles ended World War I. A punitive, but also oddly lenient, treaty was imposed on Germany. France, Britain, and the U.S. crafted a new world order based around international law and the resolution of conflict through a League of Nations. Unfortunately, there was no enforcement built into the system, and nations rapidly began disobeying its terms. Britain and the U.S., disillusioned by the war, retreated into isolationism, leaving France to take responsibility next to a badly wounded and seriously upset Germany. Europe was deeply impacted by this for two decades. Britain and France responded to the collapse of the Ottoman Empire by drawing their own map of the Middle East and splitting the remains, setting the stage for yet another anticolonial fight.

1945. In 1945, The second world war ended in the defeat of Nazi Germany and Imperial Japan. During the course of the war, however, the allies inadvertently ignited a spark of future conflict by openly arming and supporting national liberation movements where they challenged Axis foes. This broke the international consensus around the illegitimacy of revolutionary violence. Anticolonial movements began to build momentum, drawing on the rhetoric and conduct of national liberation, as laid out during WWII. The Nuremberg Trials "exploded the longstanding conceit that national policies, however odious, were to be imputed only to the nation itself and not to the individuals who shaped and enacted them" and established the concept of a "war of aggression". Thomas notes that "the implication was clear: not all wars were legitimate, and leaders could be held to account for pursuing illegitimate ones... in the space of a few traumatic years, the use of military force went from a sovereign right to an action that is illegal in all but certain narrowly defined circumstances."¹¹⁵

1967.

Cast Study – Florida Creates the Reedy Creek Improvement District

Walt Disney pushed for Reedy Creek during the initial planning of Disney World. It was

finally created the year after his death. As the intended site for the visionary Experimental Prototype Community of Tomorrow (EPCOT), Disney believed that Reedy Creek needed total autonomy and his heirs got it. The Disney Company is the effective and functional government in Reedy Creek, providing all municipal services, and subject only to county and state property taxes as well as elevator inspections.

1987.

Case Study - A.Q. Khan Network Sells Uranium Enrichment Technology to Iran

After ensuring that his own nation had the bomb, Pakistani nuclear engineer and spy Abdul Qadeer Khan, decided to sell information, sourcing, and materials. He maintained the network of suppliers he assembled to facilitate the Pakistani program and set up an independent base of operations in Dubai. He began by selling nuclear information and materials to Iran and moved on to North Korea and Libya. By the end of the 1990s, Khan's sales team "was setting up booths at arms fairs around the world and advertising his willingness to sell both conventional weapons and centrifuge technology Catalogues listed everything you needed for a nuclear program even 'complete ultracentrifuge machines'. Those who inquired were told that there would be no problem selling items to foreigners."¹¹⁶ IAEA director, general Mohammed El-Baradei, referred to this network as the "Wal-Mart of private-sector proliferation". Khan's career as the world's most prolific proliferator of nuclear weapons technology led George Tenet to describe him as "at least as dangerous as Osama bin Laden".¹¹⁷ By the time the U.S. confronted Pakistan over his activities in 2003, Khan had ensured that the world's nuclear standoff would no longer exclude the Islamic world, and accumulated a mountain of attention, power, and money.

1992. In 1992, the Soviet Union collapsed, and the bipolar international system became rapidly unipolar.

2015.

Case Study - The Wagner Group Deploys to Syria

Vladimir Putin delegated the planning of the Russian intervention in Syria to master strategist General Valery Gerasimov. In a skillfully crafted effort to avoid the failures of the Soviet invasion of Afghanistan, Gerasimov "helped craft a light footprint strategy that included a mix of airpower and maneuver elements" that kept Russian troops out of the ground war through a balance of Syrian forces, Lebanese Hezbollah, and private

114 O'Hara, *Inventing the Pinkertons, or Spies, Sleuths, Mercenaries, and Thugs: Being a Story of the Nation's Most Famous*, 2, 3.

115 Thomas, *The New Dogs of War: Nonstate Actor Violence in International Politics*, 29.

116 Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network*, 107.

117 Ibid, xii-xiv.

forces.¹¹⁸ Wagner offered the advantages of having Russian troops involved on the ground without the disadvantages of casualties, atrocities, and criminal activity, etc. These became private corporate matters and not the responsibility of the Russian government. While we have no known access to internal Wagner documents, PSMC contracts often include a clause exempting operatives from local criminal enforcement. According to one contractor, "Wagner is no ordinary private military company. It is a miniature army. We had it all, mortars, howitzers, tanks, infantry fighting vehicles and armored personnel carriers."¹¹⁹ While Gerasimov's strategy succeeded in its goal of increasing Russian power in the Middle East, there are some signs that the Russian army may have been dealing with some unintended consequences. A former Wagner mercenary who fought alongside Russians in Syria and Ukraine, told Reuters that losing the Battle of Kyiv was inevitable, since the current Russian Army has never directly fought a powerful enemy.¹²⁰ Gerasimov may have outsmarted himself by keeping his troops out of combat in Syria, as they were essentially unbloodied.

118 Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare*, 65-66.

119 Thomas, *The New Dogs of War: Nonstate Actor Violence in International Politics*, 8.

120 Reuters, *Russian troops ill-prepared for Ukraine war, says ex-Kremlin mercenary*.



APPENDIX IV

TOPICAL BIBLIOGRAPHIES

The following list of books were used to inform parts of the research (e.g., politics and cultural history) within this report and are provided for further reading, if desired.

Bibliography: Cultural History of WMDs

Daniel Barenblatt, *A Plague Upon Humanity: The Hidden History of Japan's Biological Warfare Program* (HarperCollins, 2004).

Paul Boyer, *When Time Shall Be No More: Prophecy Belief in Modern American Culture* (Harvard University Press, 1992).

Michael Bryant, *A World History of War Crimes: From Antiquity to the Present* (Bloomsbury, second edition, 2021).

Joseph Cirincione, Jon B. Wolfsthal, and Miriam Rajkumar, *Deadly Arsenal: Nuclear, Biological, and Chemical Threats*, (Carnegie Endowment for International Peace, second edition, 2005).

Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (Columbia University Press, 2007).

Eric Croddy, Clarissa Perez-Armendariz, and John Hart, *Chemical and Biological Warfare: A Comprehensive Survey for the Concerned Citizen* (Copernicus Books, 2002).

Mike Davis, *Buda's Wagon: A Brief History of the Car Bomb* (Verso, 2007).

Alex de Waal, *Mass Starvation: The History and Future of Famine* (Polity Press, 2018).

David B. Edwards, *Caravan of Martyrs: Sacrifice and Suicide Bombing in Afghanistan* (University of California Press, 2017).

Stephen Endicott and Edward Hagerman, *The United States and Biological Warfare: Secrets from the Early Cold War and Korea* (Indiana University Press, 1998).

Marie Favereau, *The Horde: How the Mongols Changed the World* (Harvard University Press, 2021).

Lawrence Freedman, *The Future of War: A History* (Public Affairs, 2017).

Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (Yale University Press, 2022).

Malcolm Gladwell, *The Bomber Mafia: A Dream, a Temptation, and the Longest Night of the Second World War* (Little, Brown, and Company, 2021).

Robert Harris and Jeremy Paxman, *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare* (Random House, 2002).

John Hershey, *Hiroshima* (Snowball Publishing, 1993; originally published in *The New Yorker*, 1946).

Fred Kaplan, *The Bomb: Presidents, Generals, and the Secret History of Nuclear War* (Simon & Schuster, 2020).

John Keegan, *A History of Warfare* (Vintage Books, 1994).

Robert J. Lifton, *Destroying the World to Save It: Aum Shinrikyo, Apocalyptic Violence, and the New Global Terrorism* (Henry Holt and Company, 2000).

Nick Lloyd, *The Western Front: A History of the Great War 1914-1918* (W.W. Norton & Company, 2021).

Paul Lockhart, *Firepower: How Weapons Shaped Warfare* (Basic Books, 2021).

Jeffrey A. Lockwood, *Six-Legged Soldiers: Using Insects as Weapons of War* (Oxford University Press, 2009).

Margaret MacMillan, *War: How Conflict Shaped Us* (Random House, 2020).

Adrienne Mayor, *Greek Fire, Poison Arrows, and Scorpion Bombs: Biological & Chemical Warfare in the Ancient World* (The Overlook Press, 2009).

Judith Miller, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War* (Simon & Schuster, 2002).

Martin Miller, *Weapons of Mass Destruction: Specters of the Nuclear Age* (Schiffer Publishing, 2017).

Nicholas Mulder, *The Economic Weapon: The Rise of Sanctions As a Tool of Modern War* (Yale University Press, 2022).

Geoffrey Parker, Ed., *The Cambridge History of Warfare* (Cambridge University Press, second edition, 2020).

Serhii Plokhy, *Nuclear Folly: A History of the Cuban Missile Crisis* (W.W. Norton & Co., 2021).

Helen E. Purkitt and Stephen F. Burgess, *South Africa's Weapons of Mass Destruction* (Indiana University Press, 2005).

Ed Regis, *The Biology of Doom: The History of America's Secret Germ Warfare Project* (Henry Holt and Company, 1999).

David Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (Broadway Books, 2018).

Eric Schlosser, *Command and Control: Nuclear Weapons, the Damascus Incident, and the Illusion of Safety* (Penguin Books, 2013).

Martin J. Sherwin, *A World Destroyed: Hiroshima and Its Legacies* (Stanford University Press, Second Edition, 2003).

Joseph M. Siracusa, *Weapons of Mass Destruction: The Search for Global Security* (Rowman & Littlefield, 2017).

Edward M. Spiers, *Agents of War: A History of Chemical and Biological Weapons* (Reaktion Books, Second Edition, 2002).

Jonathan B. Tucker, *War of Nerves: Chemical Warfare from World War I to Al-Qaeda* (New York: Random House, 2006).

Jack Weatherford, *Genghis Khan and the Making of the Modern World* (New York: Three Rivers Press, 2004).

Mark Wolverton, *Nuclear Weapons* (Cambridge, Massachusetts: MIT Press, 2022).

Bibliography: Cold War and Deterrence

Note: To avoid duplication, we have not included titles from the above WMD bibliography.

Cold War and Nations: Russia, and China

Hal Brands, *The Twilight Struggle: What the Cold War Teaches Us about Great-Power Rivalry*

Today (Yale University Press, 2022).

Michael Burleigh, *Small Wars, Faraway Places: Global Insurrection and the Making of the Modern World 1945-1965* (Penguin Books, 2013).

Campbell Craig and Sergey Radchenko, *The Atomic Bomb and the Origins of the Cold War* (Yale University Press: 2008).

Bruce Cummings, *The Korean War: A History* (Modern Library, 2011 paperback ed.).

Therese Delpech, *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Age of Strategic Piracy* (RAND, 2012).

Daniel Ellsberg, *The Doomsday Machine: Confessions of a Nuclear War Planner* (Bloomsbury, 2017).

Lawrence Freedman, *Deterrence* (Polity Press, 2004).

Lawrence Freedman and Jeffrey Michaels, *The Evolution of Nuclear Strategy* (Palgrave MacMillan, fourth edition, 2019).

John Lewis Gaddis, *The Cold War: A New History* (Penguin Books, 2005).

Francis J. Gavin, *Nuclear Statecraft: History and Strategy in America's Atomic Age* (Cornell University, 2012).

Francis J. Gavin, *Nuclear Weapons and American Grand Strategy* (Brookings Institution Press, 2020).

Max Hastings, *Vietnam: An Epic History of a Tragic War* (HarperCollins, 2018).

Jeffrey Herf, *War by Other Means: Soviet Power, West German Resistance, and the Battle of the Euromissiles* (Free Press, 1991).

David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (Anchor Books, 2009).

David Holloway, *Stalin and the Bomb* (Yale University Press, 1994).

Seth G. Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (W.W. Norton, 2021).

Tony Judt, *Postwar: A History of Europe Since 1945* (Penguin Books, 2006).

Jeffrey Lewis, *Paper Tigers: China's Nuclear Posture* (International Institute for Strategic Studies, 2014).

John Wilson Lewis and Xue Litai, *China Builds the Bomb* (Stanford University Press, 1988).

Kier A. Lieber and Daryl G. Press, *The Myth of the Nuclear Revolution: Power Politics in the Atomic Age* (Cornell University Press, 2020).

Priscilla J. McMillan, *The Ruin of Robert J. Oppenheimer and the Birth of the Modern Arms Race* (Johns Hopkins Press, second edition, 2018).

M.E. Sarotte, *Not One Inch: America, Russia, and the Making of Post-Cold War Stalemate* (Yale University Press, 2021).

James M. Smith and Paul J. Bolt, *China's Strategic Arsenal: Worldview, Doctrine, and Systems* (Georgetown University Press, 2021).

Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945* (Cambridge University Press, 2007).

Marc Trachtenberg, *A Constructed Peace: The Making of the European Settlement, 1945-1963* (Princeton University Press, 1999).

Toshi Yoshihara and James R. Holmes, Eds., *Strategy in the Second Nuclear Age: Power, Ambition, and the Ultimate Weapon* (Georgetown University Press, 2012).

Vadislav M. Zubok, *Collapse: The Fall of the Soviet Union* (Yale University Press, 2021).

Other Nations: India, Israel, North Korea, Pakistan

Hassan Abbas, *Pakistan's Nuclear Bomb: A Story of Deterrence and Deviance* (Oxford University Press, 2018).

Sanjay Badri-Maharaj, *Nuclear India: From Reluctance to Triad* (Helion and Company, 2021).

Avner Cohen, *The Worst-Kept Secret: Israel's Bargain with the Bomb* (Columbia University Press, 2010).

Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network* (Oxford University Press, 2006).

Michael Karpin, *The Bomb in the Basement: How Israel Went Nuclear and What That Means for the World* (Simon & Schuster, 2006).

Feroz Hassan Khan, *Eating Grass: The Making of the Pakistani Bomb* (Stanford University Press, 2012).

Sung Chull Kim and Michael D. Cohen, Eds., *North Korea and Nuclear Weapons: Entering the New Era of Deterrence* (Georgetown University Press, 2017).

Mahdi Obeidi and Kurt Pitzer, *The Bomb in My Garden: The Secrets of Saddam's Nuclear Mastermind* (John Wiley and Sons, 2004).

Zaki Shalom, *Israel's Nuclear Option: Behind the Scenes Diplomacy between Dimona and Washington* (Sussex Academic Press, Second Edition, 2012).

Bibliography: Non-Nation State Actors

Stephen Biddle, *Nonstate Warfare: The Military Methods of Guerrillas, Warlords, and Militias* (Princeton: Princeton University Press, 2021).

Erica Chenoweth and Adria Lawrence, Eds., *Rethinking Violence: States and Non-State Actors in Conflict* (Cambridge: MIT Press, 2010).

N.W. Collins, *Grey Wars: A Contemporary History of U.S. Special Operations* (New Haven: Yale University Press, 2021).

William Dalrymple, *The Anarchy: The East India Company, Corporate Violence, and the Pillage of an Empire* (New York: Bloomsbury Publishing, 2019).

Richard English, *Armed Struggle: The History of the IRA* (New York: Oxford University Press, 2003).

Natasha Ezrow, *Global Politics and Violent Non-State Actors* (Los Angeles: Sage Publishing, 2017).

Fawaz A. Gerges, *ISIS: A History* (Princeton: Princeton University Press, 2016).

Linda Gordon, *The Second Coming of the KKK: The Ku Klux Klan of the 1920s and the American Political Tradition* (New York: Liveright Publishing, 2017).

Jacob J. Grygiel, *Return of the Barbarians: Confronting Non-State Actors from Ancient Rome to the Present* (New York, Cambridge University Press, 2018).

Richard Haas, *The World: A Brief Introduction* (New York: Penguin Books, 2020).

Tony Horwitz, *Confederates in the Attic: Dispatches from the Unfinished Civil War* (New York: Pantheon Books, 1998).

Seth G. Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (New York: W.W. Norton & Company, 2021).

Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era* (Stanford: Stanford University Press, Third Edition, 2012).

Henry Kissinger, *World Order* (New York: Penguin Books, 2014).

Charles Lister and Paul Salem, Eds., *Winning the Battle, Losing the War: Addressing the Drivers Fueling Armed Non-State Actors and Extremist Groups* (Washington: The Middle East Institute, 2019).

Kimberly Marten, *Warlords: Strong-Arm Brokers in Weak States* (Ithaca: Cornell University Press, 2012).

S. Paul O'Hara, *Inventing the Pinkertons, or Spies, Sleuths, Mercenaries, and Thugs: Being a Story of the Nation's Most Famous (and Infamous) Detective Agency* (Baltimore: John Hopkins Press, 2016).

Andrew Phillips and J.C. Sharman, *Outsourcing Empire: How Company-States Made the Modern World* (Princeton: Princeton University Press, 2020).

Gary Schaub, Jr. and Ryan Kelty, Eds. *Private Military and Security Contractors: Controlling the Corporate Warrior* (New York: Rowman & Littlefield, 2016).

Emile Simpson, *War from the Ground Up: Twenty-First-Century Combat As Politics* (New York: Oxford University Press, 2018).

Philip J. Stern, *The Company-State: Corporate Sovereignty & the Early Modern Foundations of the British Empire in India* (New York: Oxford University Press, 2011).

Ward Thomas, *The New Dogs of War: Nonstate Actor Violence in International Politics* (Ithaca: Cornell University Press, 2021).

Janice E. Thompson, *Mercenaries, Pirates, & Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe* (Princeton: Princeton University Press, 1994).



Visit threatcasting.com for more information

